23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

10. Which type of attack takes place when you leave your phone's Bluetooth setting as discoverable and someone takes control of your phone and connects it to the Internet?

a. evil twin [Incorrect. An evil twin is a wireless network with the same name as another wireless access point, allowing hackers to collect sensitive information.]

► **b.** bluebugging [Correct.]

c. internet terrorism [Incorrect. Internet terrorism is using the internet to disrupt communications and e-commerce.]

d. bluesnarfing [Incorrect. Bluesnarfing is using Bluetooth to steal contact lists, calendars, pictures, etc.]

https://fliphtml5.com/pyiue/oxby/basic/301-350 1/45

CHAPTER

10

Control and Accounting Information Systems

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

1. Explain basic control concepts and explain why computer control and security are important.
2. Compare and contrast the COBIT, COSO, and ERM control frameworks.
3. Describe the major elements in the control environment of a company.
4. Describe the control objectives companies need to set and how to identify threats that affect organizational uncertainty.
5. Explain how to assess and respond to risk using the Enterprise Risk Management (ERM) model.
6. Describe control activities commonly used in companies.
7. Describe how to communicate information and monitor control processes in organizations.

INTEGRATIVE CASE Springer's Lumber & Supply

Jason Scott, an internal auditor for Northwest Industries, is auditing Springer's Lumber & Supply, Northwest's building materials outlet in Bozeman, Montana. His supervisor, Maria Pilier, asked him to trace a sample of purchase transactions from purchase requisition to cash disbursement to verify that proper control procedures were followed. Jason is frustrated with this task, and for good reasons:

- The purchasing system is poorly documented.
- He keeps finding transactions that have not been processed as Ed Yates, the accounts payable manager, said they should be.
- Purchase requisitions are missing for several items personally authorized by Bill Springer, the purchasing vice president.
- Some vendor invoices have been paid without supporting documents, such as purchase orders and receiving reports.

Petr Vaclavek/Shutterstock

- Prices for some items seem unusually high, and there are a few discrepancies in item prices between the vendor invoice and the corresponding purchase order.

Yates had a logical answer for every question Jason raised and advised Jason that the real world is not as tidy as the world portrayed in college textbooks. Maria also has some concerns:

- Springer's is the largest supplier in the area and has a near monopoly.
- Management authority is held by the company president, Joe Springer, and his two sons, Bill (the purchasing vice president) and Ted (the controller). Several relatives and friends are on the payroll. Together, the Springers own 10% of the company.
- Lines of authority and responsibility within the company are loosely defined and confusing.
- Maria believes that Ted Springer may have engaged in "creative accounting" to make Springer's one of Northwest's best-performing retail outlets.

After talking to Maria, Jason ponders the following issues:

1. Because Ed Yates had a logical explanation for every unusual transaction, should Jason describe these transactions in his report?
2. Is a violation of control procedures acceptable if management has authorized it?
3. Maria's concerns about Springer's loosely defined lines of authority and possible use of "creative accounting" are matters of management policy. With respect to Jason's control procedures assignment, does he have a professional or an ethical responsibility to get involved?

Introduction

WHY THREATS TO ACCOUNTING INFORMATION SYSTEMS ARE INCREASING

In most years, more than 60% of organizations experience a major failure in controlling the security and integrity of their computer systems. Reasons for the failures include the following:

- Information is available to an unprecedented number of workers. Chevron, for example, has more than 35,000 PCs.
- Information on distributed computer networks is hard to control. At Chevron, information is distributed among many systems and thousands of employees worldwide. Each system and each employee represent a potential control vulnerability point.
- Customers and suppliers have access to each other's systems and data. For example, Walmart allows vendors to access their databases. Imagine the confidentiality problems as these vendors form alliances with Walmart competitors.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

Organizations have not adequately protected data for several reasons:

- Some companies view the loss of crucial information as a distant, unlikely threat.
- The control implications of moving from centralized computer systems to Internet-based systems are not fully understood.
- Many companies do not realize that information is a strategic resource and that protecting it must be a strategic requirement. For example, one company lost millions of dollars because it did not protect data transmissions. A competitor tapped into its phone lines and obtained faxes of new product designs.
- Productivity and cost pressures motivate management to forgo time-consuming control measures.

threat - Any potential adverse occurrence or unwanted event that could injure the AIS or the organization.

Any potential adverse occurrence is called a **threat**. The potential dollar loss from a threat is called the **exposure/impact**. The probability that it will happen is called the **likelihood/risk** of the threat.

exposure/impact - The potential dollar loss if a particular threat becomes a reality.

likelihood/risk - The probability that a threat will come to pass.

Overview of Control Concepts

internal controls - The processes and procedures implemented to provide reasonable assurance that control objectives are met.

Internal controls are the processes implemented to provide reasonable assurance that the following control objectives are achieved:

- Safeguard assets—prevent or detect their unauthorized acquisition, use, or disposition.
- Maintain records in sufficient detail to report company assets accurately and fairly.
- Provide accurate and reliable information.
- Prepare financial reports in accordance with established criteria.
- Promote and improve operational efficiency.
- Encourage adherence to prescribed managerial policies.
- Comply with applicable laws and regulations.

Internal control is a process because it permeates an organization's operating activities and is an integral part of management activities. Internal control provides reasonable assurance—complete assurance is difficult to achieve and prohibitively expensive. In addition, internal control systems have inherent limitations, such as susceptibility to simple errors and mistakes, faulty judgments and decision making, management overrides, and collusion.

Developing an internal control system requires a thorough understanding of information technology (IT) capabilities and risks, as well as how to use IT to achieve an organization's control objectives. Accountants and systems developers help management achieve their control objectives by (1) designing effective control systems that take a proactive approach to eliminating system threats and that detect, correct, and recover from threats when they occur; and (2) making it easier to build controls into a system at the initial design stage than to add them after the fact.

preventive controls - Controls that deter problems before they arise.

detective controls - Controls designed to discover control problems that were not prevented.

corrective controls - Controls that identify and correct problems as well as correct and recover from the resulting errors.

Internal controls perform three important functions:

1. **Preventive controls** deter problems before they arise. Examples include hiring qualified personnel, segregating employee duties, and controlling physical access to assets and information.
2. **Detective controls** discover problems that are not prevented. Examples include duplicate checking of calculations and preparing bank reconciliations and monthly trial balances.
3. **Corrective controls** identify and correct problems as well as correct and recover from the resulting errors. Examples include maintaining backup copies of files, correcting data entry errors, and resubmitting transactions for subsequent processing.

general controls - Controls designed to make sure an organization's information system and control environment is stable and well managed.

application controls - Controls that prevent, detect, and correct transaction errors and fraud in application programs.

Internal controls are often segregated into two categories:

1. **General controls** make sure an organization's control environment is stable and well managed. Examples include security; IT infrastructure; and software acquisition, development, and maintenance controls.
2. **Application controls** prevent, detect, and correct transaction errors and fraud in application programs. They are concerned with the accuracy, completeness, validity, and authorization of the data captured, entered, processed, stored, transmitted to other systems, and reported.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

Robert Simons, a Harvard business professor, has espoused four levers of control to help management reconcile the conflict between creativity and controls.

1. A **belief system** describes how a company creates value, helps employees understand management's vision, communicates company core values, and inspires employees to live by those values.
2. A **boundary system** helps employees act ethically by setting boundaries on employee behavior. Instead of telling employees exactly what to do, they are encouraged to creatively solve problems and meet customer needs while meeting minimum performance standards, shunning off-limit activities, and avoiding actions that might damage their reputation.
3. A **diagnostic control system** measures, monitors, and compares actual company progress to budgets and performance goals. Feedback helps management adjust and fine-tune inputs and processes so future outputs more closely match goals.
4. An **interactive control system** helps managers to focus subordinates' attention on key strategic issues and to be more involved in their decisions. Interactive system data are interpreted and discussed in face-to-face meetings of superiors, subordinates, and peers.

belief system - System that describes how a company creates value, helps employees understand management's vision, communicates company core values, and inspires employees to live by those values.

boundary system - System that helps employees act ethically by setting boundaries on employee behavior.

diagnostic control system - System that measures, monitors, and compares actual company progress to budgets and performance goals.

interactive control system - System that helps managers to focus subordinates' attention on key strategic issues and to be more involved in their decisions.

Regrettably, not all organizations have an effective internal control system. For instance, one report indicated that the FBI is plagued by IT infrastructure vulnerabilities and security problems, some of which were identified in an audit 16 years previously. Specific areas of concern were security standards, guidelines, and procedures; segregation of duties; access controls, including password management and usage; backup and recovery controls; and software development and change controls.

THE FOREIGN CORRUPT PRACTICES AND SARBANES–OXLEY ACTS

In 1977, the **Foreign Corrupt Practices Act (FCPA)** was passed to prevent companies from bribing foreign officials to obtain business. Congress incorporated language from an American Institute of Certified Public Accountants (AICPA) pronouncement into the FCPA that required corporations to maintain good systems of internal control. Unfortunately, these requirements were not sufficient to prevent further problems.

Foreign Corrupt Practices Act (FCPA) - Legislation passed to prevent companies from bribing foreign officials to obtain business; also requires all publicly owned corporations maintain a system of internal accounting controls.

Companies who violate the FCPA are subject to fines. Recently, a large multinational U.S. bank agreed to pay a $264 million fine for allegedly hiring the children of Chinese rulers, who were not qualified for the jobs they were given, to win business from the Chinese government. Another example is Odebrecht, a Brazilian conglomerate, who was required to pay a record $2.6 billion fine to Brazil, the United States, and Switzerland for paying kickbacks to government officials and Petrobras management in return for oil and gas contracts. The corruption was so bad that authorities set the fine amount as high as they thought it was possible for Odebrecht to pay without having to declare bankruptcy. In the aftermath of the Petrobras corruption scandal, Odebrecht's CEO was sentenced to 19 years in jail and Brazil's president was impeached.

In the late 1990s and early 2000s, news stories were reporting accounting frauds at Enron, WorldCom, Xerox, Tyco, Global Crossing, Adelphia, and other companies. When Enron, with $62 billion in assets, declared bankruptcy in December 2001, it was the largest bankruptcy in U.S. history. In June 2002, Arthur Andersen, once the largest CPA firm, collapsed. The Enron bankruptcy was dwarfed when WorldCom, with more than $100 billion in assets, filed for bankruptcy in July 2002. In response to these frauds, Congress passed the **Sarbanes–Oxley Act (SOX)** of 2002. SOX applies to publicly held companies and their auditors and was designed to prevent financial statement fraud, make financial reports more transparent, protect investors, strengthen internal controls, and punish executives who perpetrate fraud.

Sarbanes–Oxley Act (SOX) - Legislation intended to prevent financial statement fraud, make financial reports more transparent, provide protection to investors, strengthen internal controls at public companies, and punish executives who perpetrate fraud.

SOX is the most important business-oriented legislation in the last 80 years. It changed the way boards of directors and management operate and had a dramatic impact on CPAs who audit them. The following are some of the most important aspects of SOX:

- **Public Company Accounting Oversight Board (PCAOB).** SOX created the **Public Company Accounting Oversight Board (PCAOB)** to control the auditing profession. The PCAOB sets and enforces auditing, quality control, ethics, independence, and other auditing standards. It consists of five people who are appointed by the Securities and Exchange Commission (SEC).

Public Company Accounting Oversight Board (PCAOB) - A board created by SOX that regulates the auditing profession; created as part of SOX.

https://fliphtml5.com/pyiue/oxby/basic/301-350 5/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

- **New rules for auditors.** Auditors must report specific information to the company's audit committee, such as critical accounting policies and practices. SOX prohibits auditors from performing certain nonaudit services, such as information systems design and implementation. Audit firms cannot provide services to companies if top management was employed by the auditing firm and worked on the company's audit in the preceding 12 months.
- **New roles for audit committees.** Audit committee members must be on the company's board of directors and be independent of the company. One member of the audit committee must be a financial expert. The audit committee hires, compensates, and oversees the auditors, who report directly to them.
- **New rules for management.** SOX requires the CEO and CFO to certify that (1) financial statements and disclosures are fairly presented, were reviewed by management, and are not misleading; and that (2) the auditors were told about all material internal control weaknesses and fraud. If management knowingly violates these rules, they can be prosecuted and fined. Companies must disclose, in plain English, material changes to their financial condition on a timely basis.
- **New internal control requirements.** Section 404 requires companies to issue a report accompanying the financial statements stating that management is responsible for establishing and maintaining an adequate internal control system. The report must contain management's assessment of the company's internal controls, attest to their accuracy, and report significant weaknesses or material noncompliance.

After SOX was passed, the SEC mandated that management must:

- Base its evaluation on a recognized control framework. The most likely frameworks, formulated by the Committee of Sponsoring Organizations (COSO), are discussed in this chapter.
- Disclose all material internal control weaknesses.
- Conclude that a company does not have effective financial reporting internal controls if there are material weaknesses.

Control Frameworks

This section discusses three frameworks used to develop internal control systems.

COBIT FRAMEWORK

Control Objectives for Information and Related Technology (COBIT) - A security and control framework that allows (1) management to benchmark the security and control practices of IT environments, (2) users of IT services to be assured that adequate security and control exist, and (3) auditors to substantiate their internal control opinions and advise on IT security and control matters.

The Information Systems Audit and Control Association (ISACA) developed the **Control Objectives for Information and Related Technology (COBIT)** framework. COBIT consolidates control standards from many different sources into a single framework that allows (1) management to benchmark security and control practices of IT environments, (2) users to be assured that adequate IT security and controls exist, and (3) auditors to substantiate their internal control opinions and to advise on IT security and control matters.

The COBIT 2019 framework describes best practices for the effective governance and management of IT. COBIT 2019 is based on the following five key principles of IT governance and management. These principles help organizations build an effective governance and management framework that protects stakeholders' investments and produces the best possible information system.

1. **Meeting stakeholder needs.** This helps users customize business processes and procedures to create an information system that adds value to its stakeholders. It also allows the company to create the proper balance between risk and reward.
2. **Covering the enterprise end-to-end.** This does not just focus on the IT operation, it integrates all IT functions and processes into companywide functions and processes.

https://fliphtml5.com/pyiue/oxby/basic/301-350 6/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

3. **Applying a single, integrated framework.** This can be aligned at a high level with other standards and frameworks so that an overarching framework for IT governance and management is created.
4. **Enabling a holistic approach.** This provides a holistic approach that results in effective governance and management of all IT functions in the company.
5. **Separating governance from management.** This distinguishes between governance and management.

As shown in Figure 10-1, there are five governance and management objectives in COBIT 2019. The objective of governance is to create value by optimizing the use of organizational resources to produce desired benefits in a manner that effectively addresses risk. Governance is the responsibility of the board of directors who (1) evaluate stakeholder needs to identify objectives, (2) provide management with direction by prioritizing objectives, and (3) monitor management's performance.

Management is responsible for planning, building, running, and monitoring the activities and processes used by the organization to pursue the objectives established by the board of directors. Management also periodically provides the board of directors with feedback that can be used to monitor achievement of the organization's objectives and, if necessary, to re-evaluate and perhaps modify those objectives.

The governance and management of IT are ongoing processes. The board of directors and management monitor the organization's activities and use that feedback to modify existing plans and procedures or develop new strategies to respond to changes in business objectives and new developments in IT.

COBIT 2019 is a comprehensive framework that helps enterprises achieve their IT governance and management objectives. This comprehensiveness is one of the strengths of COBIT 2019 and underlies its growing international acceptance as a framework for managing and controlling information systems.

Figure 10-2 is the COBIT 2019 process reference model. The model identifies the five governance processes (referred to as evaluate, direct and monitor—or EDM) and 35 management processes. The 35 management processes are broken down into the following four domains:

1. Align, plan, and organize (APO).
2. Build, acquire, and implement (BAI).
3. Deliver, service, and support (DSS).
4. Monitor, evaluate, and assess (MEA).

It is not possible to cover all of COBIT 2019 in this text. Instead, in Chapters 11 through 13 we focus on the portions of COBIT 2019 most directly relevant to accountants, auditors, and accounting information systems. This includes the business processes and control activities that affect the accuracy of an organization's financial statements and its compliance with external regulations such as SOX, the Health Insurance Portability and Accountability Act (HIPAA), and the security standards mandated by the credit card industry.

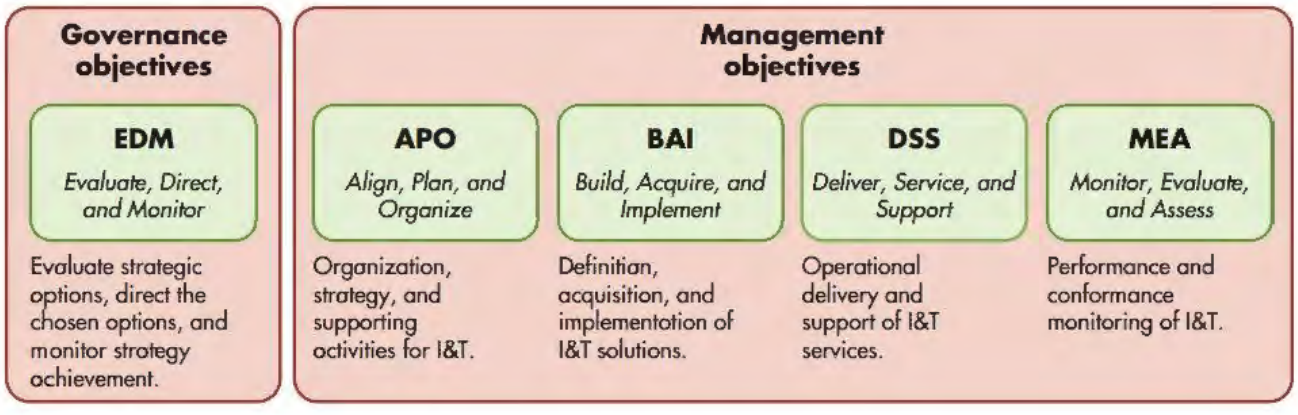


FIGURE 10-1
COBIT 2019 Governance and Management Objectives
COBIT® 2019. © 2019 ISACA® All rights reserved. Used by permission of ISACA.

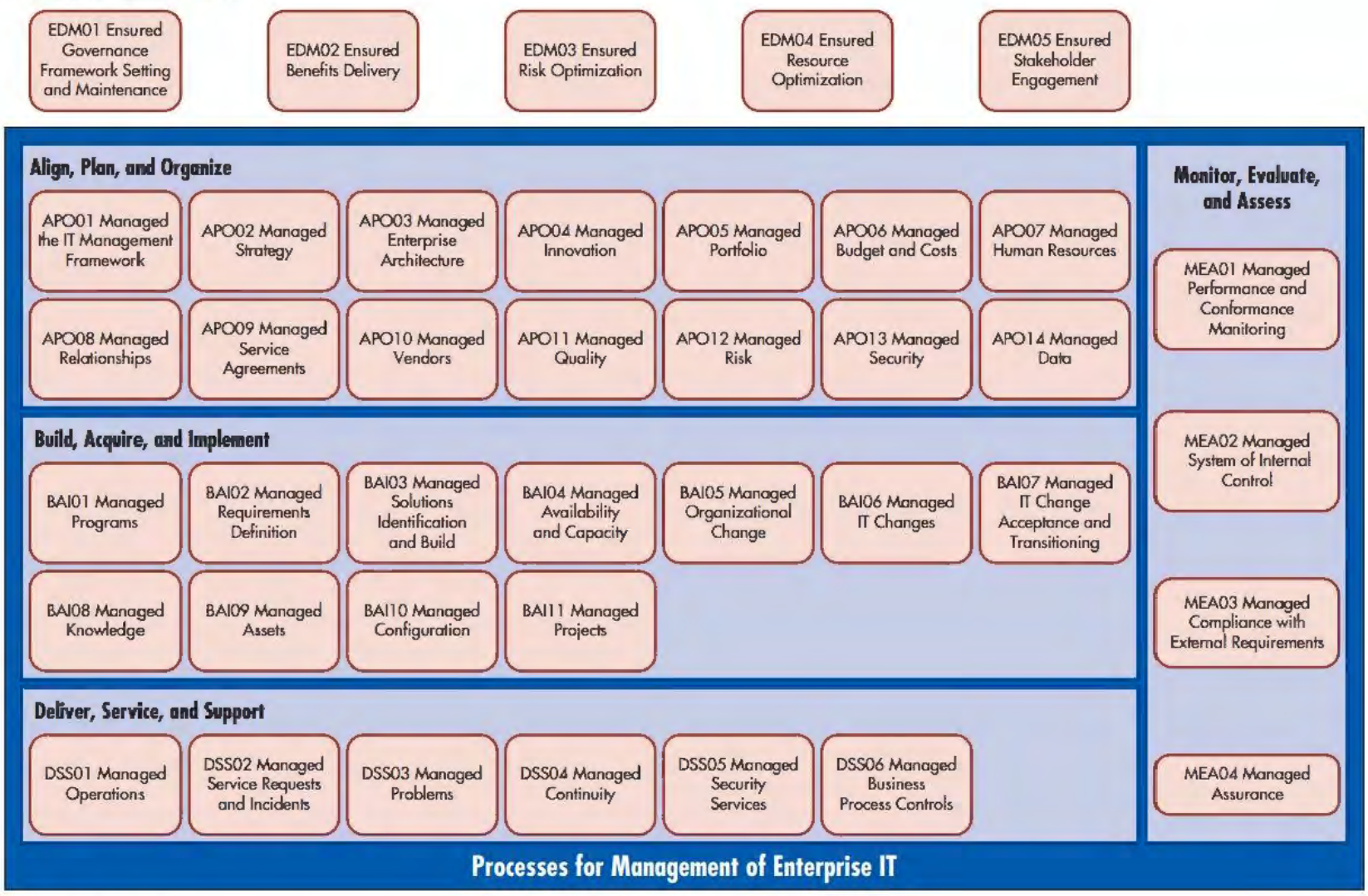

Processes for Governance of Enterprise IT
Evaluate, Direct, and Monitor
EDM01 Ensured Governance Framework Setting and Maintenance
EDM02 Ensured Benefits Delivery
EDM03 Ensured Risk Optimization
EDM04 Ensured Resource Optimization
EDM05 Ensured Stakeholder Engagement
Align, Plan, and Organize
APO01 Managed the IT Management Framework
APO02 Managed Strategy
APO03 Managed Enterprise Architecture
APO04 Managed Innovation
APO05 Managed Portfolio
APO06 Managed Budget and Costs
APO07 Managed Human Resources
APO08 Managed Relationships
APO09 Managed Service Agreements
APO10 Managed Vendors
APO11 Managed Quality
APO12 Managed Risk
APO13 Managed Security
APO14 Managed Data
Build, Acquire, and Implement
BAI01 Managed Programs
BAI02 Managed Requirements Definition
BAI03 Managed Solutions Identification and Build
BAI04 Managed Availability and Capacity
BAI05 Managed Organizational Change
BAI06 Managed IT Changes
BAI07 Managed IT Change Acceptance and Transitioning
BAI08 Managed Knowledge
BAI09 Managed Assets
BAI10 Managed Configuration
BAI11 Managed Projects
Deliver, Service, and Support
DSS01 Managed Operations
DSS02 Managed Service Requests and Incidents
DSS03 Managed Problems
DSS04 Managed Continuity
DSS05 Managed Security Services
DSS06 Managed Business Process Controls
Monitor, Evaluate, and Assess
MEA01 Managed Performance and Conformance Monitoring
MEA02 Managed System of Internal Control
MEA03 Managed Compliance with External Requirements
MEA04 Managed Assurance
Processes for Management of Enterprise IT

FIGURE 10-2

COBIT 2019 Process Reference Model

COBIT® 2019. © 2019 ISACA® All rights reserved. Used by permission from ISACA.

COSO'S INTERNAL CONTROL FRAMEWORK

Committee of Sponsoring Organizations (COSO) - A private-sector group consisting of the American Accounting Association, the AICPA, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.

Internal Control—Integrated Framework (IC) - A COSO framework that defines internal controls and provides guidance for evaluating and enhancing internal control systems.

The **Committee of Sponsoring Organizations (COSO)** consists of the American Accounting Association, the AICPA, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute. In 1992, COSO issued **Internal Control—Integrated Framework (IC)**, which is widely accepted as the authority on internal controls and is incorporated into policies, rules, and regulations used to control business activities.

In 2013, the IC framework was updated to better deal with current business processes and technological advancements. For example, in 1992, very few businesses used the Internet, sent e-mail, or stored their data in the cloud. The revised IC framework also provides users with more precise guidance on how to implement and document the framework. Many new examples have been added to clarify framework concepts and make the framework easier to understand and use. The new IC framework keeps the five components of the original framework and adds 17 principles that build on and support the concepts. Each of the five components has at least two and up to five principles.

The five components and 17 principles of the IC framework are summarized in Table 10-1. Because COSO Internal Control—Integrated Framework is the most commonly used control framework, the text uses it to explain internal controls. Focus 10-1 explains other COSO control frameworks.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

FOCUS 10-1 COSO's Enterprise Risk Management Frameworks

Enterprise Risk Management—Integrated Framework (ERM)

To improve the risk management process, in 2004 COSO developed a second control framework called Enterprise Risk Management—Integrated Framework (ERM). ERM is the process the board of directors and management use to set strategy, identify events that may affect the entity, assess and manage risk, and provide reasonable assurance that the company achieves its objectives and goals. The basic principles behind ERM are as follows:

- Companies are formed to create value for their owners.
- Management must decide how much uncertainty it will accept as it creates value.
- Uncertainty results in risk, which is the possibility that something negatively affects the company's ability to create or preserve value.
- Uncertainty results in opportunity, which is the possibility that something positively affects the company's ability to create or preserve value.
- The ERM framework can manage uncertainty as well as create and preserve value.

Enterprise Risk Management—Integrating with Strategy and Performance

After ERM was published, new risks emerged and the complexity of existing risk changed. To address this, the ERM framework was updated in 2017 and retitled Enterprise Risk Management—Integrating with Strategy and Performance. The new title recognizes and highlights how important it is to consider risk in setting company strategy and in helping companies improve their performance. The new framework contains 20 control principles that are divided into the following five interrelated components:

1. **Governance and Culture:** Governance sets the organization's tone, including oversight responsibilities for enterprise risk management. Culture relates to a company's ethical values, desired behaviors, and understanding of risk.
2. **Strategy and Objective Setting:** Strategic planning should include corporate strategy, objective setting, and enterprise risk management. A company's appetite for risk should be aligned with strategy. Business objectives should be created to put strategy into practice. Strategies and business objectives should consider the need to identify, assess, and respond to risk.
3. **Performance:** Entities should identify and assess the risks that affect its strategy and business objectives, prioritize them based on their risk appetite, and determine how to respond to each risk. The risk response process should include an assessment of the total amount of risk the entity assumes. Key risk stakeholders should be informed of the risk assessment and response process and its findings.
4. **Review and Revision:** The entity should review the performance of ERM components to determine how well they are functioning over time, and determine what revisions are needed.
5. **Information, Communication, and Reporting:** It is essential to continuously obtain and share information from internal and external sources with all necessary levels of the organization.

The control principles in the five components cover all aspects of enterprise risk that can accommodate different viewpoints and operating structures. Adhering to them provides stakeholders, management, and the board with a reasonable expectation that the entity understands and is managing strategy and business objective risks.

Improving Organizational Resiliency: New Guidance Addresses Environmental, Social, and Governance-related Risks (ESG)

In 2018, COSO released new ERM guidance: Improving Organizational Resiliency: New Guidance Addresses Environmental, Social, and Governance-Related Risks (ESG). ESG-related risks are increasing in number and severity world-wide, raising demand for ESG-related insight. The ESG guidance was designed to be easily integrated with COSO's Enterprise Risk Management—Integrating with Strategy and Performance guidance. The ESG documentation includes:

- Methods for overcoming ESG risks related to all five of ERM's components.
- Ways to manage ESG risks.
- Methods for managing ESG risks by developing and maintaining a continuous improvement culture.

The ERM Framework versus the Internal Control Framework

The IC framework has been widely adopted as the way to evaluate internal controls, as required by SOX. The more comprehensive ERM frameworks take a risk-based approach rather than a controls-based approach. ERM controls are flexible and relevant because they are linked to current organizational objectives. The ERM model also recognizes that risk, in addition to being controlled, can be accepted, avoided, diversified, shared, or transferred.

https://fliphtml5.com/pyiue/oxby/basic/301-350 9/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

TABLE 10-1 Five Components and 17 Principles of COSO's Internal Control Model

Component	Description
Control environment	This is the foundation for all other components of internal control. The core of any business is its people—their individual attributes, including integrity, discipline, ethical values, and competence—and the environment in which they operate. They are the engine that drives the organization and the foundation on which everything rests. 1. Commitment to integrity and ethics 2. Internal control oversight by the board of directors, independent of management 3. Structures, reporting lines, and appropriate responsibilities in the pursuit of objectives established by management and overseen by the board 4. A commitment to attract, develop, and retain competent individuals in alignment with objectives 5. Holding individuals accountable for their internal control responsibilities in pursuit of objectives
Risk assessment	The organization must identify, analyze, and manage its risks. Managing risk is a dynamic process. Management must consider changes in the external environment and within the business that may be obstacles to its objectives. 6. Specifying objectives clearly enough for risks to be identified and assessed 7. Identifying and analyzing risks to determine how they should be managed 8. Considering the potential of fraud 9. Identifying and assessing changes that could significantly impact the system of internal control
Control activities	Control policies and procedures help ensure that the actions identified by management to address risks and achieve the organization's objectives are effectively carried out. Control activities are performed at all levels and at various stages within the business process and over technology. 10. Selecting and developing controls that might help mitigate risks to an acceptable level 11. Selecting and developing general control activities over technology 12. Deploying control activities as specified in policies and relevant procedures
Information and communication	Information and communication systems capture and exchange the information needed to conduct, manage, and control the organization's operations. Communication must occur internally and externally to provide information needed to carry out day-to-day internal control activities. All personnel must understand their responsibilities. 13. Obtaining or generating relevant, high-quality information to support internal control 14. Internally communicating information, including objectives and responsibilities, necessary to support the other components of internal control 15. Communicating relevant internal control matters to external parties
Monitoring	The entire process must be monitored, and modifications made as necessary so the system can change as conditions warrant. Evaluations ascertain whether each component of internal control is present and functioning. Deficiencies are communicated in a timely manner, with serious matters reported to senior management and the board. 16. Selecting, developing, and performing ongoing or separate evaluations of the components of internal control 17. Evaluating and communicating deficiencies to those responsible for corrective action, including senior management and the board of directors, where appropriate

The Control Environment

control environment - The company culture that is the foundation for all other internal control components, as it influences how organizations establish strategies and objectives; structure business activities; and identify, assess, and respond to risk.

The **control environment**, or company culture, influences how organizations establish strategies and objectives; structure business activities; and identify, assess, and respond to risk. It is the foundation for all other ERM components. A weak or deficient control environment often results in breakdowns in risk management and control. It is essentially the same thing as the control environment in the IC framework.

A control environment consists of the following:

1. Management's philosophy, operating style, and risk appetite.
2. Commitment to integrity, ethical values, and competence.
3. Internal control oversight by the board of directors.
4. Organizational structure.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

5. Methods of assigning authority and responsibility.
6. Human resource standards that attract, develop, and retain competent individuals.
7. External influences.

Enron is an example of an ineffective control environment that resulted in financial failure. Although Enron appeared to have an effective ERM system, its control environment was defective. Management engaged in risky and dubious business practices, which the board of directors never questioned. Management misrepresented the company's financial condition, lost the confidence of shareholders, and finally filed for bankruptcy.

MANAGEMENT'S PHILOSOPHY, OPERATING STYLE, AND RISK APPETITE

Collectively, an organization has a philosophy, or shared beliefs and attitudes, about risk that affects policies, procedures, oral and written communications, and decisions. Companies also have a **risk appetite**, which is the amount of risk they are willing to accept to achieve their goals. To avoid undue risk, risk appetite must be in alignment with company strategy.

risk appetite - The amount of risk a company is willing to accept to achieve its goals and objectives. To avoid undue risk, risk appetite must be in alignment with company strategy.

The board of directors and top management must set the proper tone at the top; that is, they need to demonstrate through their actions that they support integrity and the necessity for a strong internal control system. The more responsible management's philosophy and operating style, and the more clearly they are communicated, the more likely employees will behave responsibly. If management has little concern for internal controls and risk management, then employees are less diligent in achieving control objectives. The culture at Springer's Lumber & Supply provides an example. Maria Pilier found that lines of authority and responsibility were loosely defined and suspected management might have used "creative accounting" to improve company performance. Jason Scott found evidence of poor internal control practices in the purchasing and accounts payable functions. These two conditions may be related; management's loose attitude may have contributed to the purchasing department's inattentiveness to good internal control practices.

Management's philosophy, operating style, and risk appetite can be assessed by answering questions such as these:

- Does management take undue business risks to achieve its objectives, or does it assess potential risks and rewards prior to acting?
- Does management manipulate performance measures, such as net income, so they are seen in a more favorable light?
- Does management pressure employees to achieve results regardless of the methods, or does it demand ethical behavior? In other words, do the ends justify the means?

COMMITMENT TO INTEGRITY, ETHICAL VALUES, AND COMPETENCE

Organizations need a culture that stresses integrity and commitment to ethical values and competence. Ethics pays—ethical standards are good business. Integrity starts at the top, as company employees adopt top management attitudes about risks and controls. A powerful message is sent when the CEO, confronted with a difficult decision, makes the ethically correct choice.

Companies endorse integrity by:

- Developing a written code of conduct that explicitly describes honest and dishonest behaviors. For example, most purchasing agents agree that accepting $5,000 from a supplier is dishonest, but a weekend vacation is not as clear-cut. A major cause of dishonesty comes from rationalizing unclear situations and allowing the criterion of expediency to replace the criterion of right versus wrong. Companies should document that employees have read and understand the code of conduct.
- Put processes in place to use the company's code of conduct to evaluate individual and team performance and to address any deviations in a timely and consistent manner.
- Actively teaching and requiring the code of conduct—for example, making it clear that honest reports are more important than favorable ones.
- Avoiding unrealistic expectations or incentives that motivate dishonest or illegal acts, such as overly aggressive sales practices, unfair or unethical negotiation tactics, and bonuses excessively based on reported financial results.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

- Consistently rewarding honesty and giving verbal labels to honest and dishonest behavior. If companies punish or reward honesty without labeling it as such, or if the standard of honesty is inconsistent, then employees will display inconsistent moral behavior.
- Requiring employees to report dishonest or illegal acts and disciplining employees who knowingly fail to report them. All dishonest acts should be investigated, and dishonest employees should be dismissed and prosecuted to show that such behavior is not allowed.
- Making a commitment to competence. Companies should hire competent employees with the necessary knowledge, experience, training, and skills.

INTERNAL CONTROL OVERSIGHT BY THE BOARD OF DIRECTORS

An involved board of directors represents shareholders and provides an independent review of management that acts as a check and balance on its actions. It is important that the board approve company strategy and review security policies. The board should also evaluate management and management decision making. To do so, the board needs members with the skills and expertise necessary to ask senior management probing questions. They also need enough members who are independent of management so the board can objectively evaluate them. If needed, the board should supplement their expertise by hiring outside consultants. For example, they may need help evaluating the security, processing integrity, availability, confidentiality, and privacy of the company's information systems. The board must also be willing and able to take any needed actions to protect the company's shareholders.

audit committee - The outside, independent board of director members responsible for financial reporting, regulatory compliance, internal control, and hiring and overseeing internal and external auditors.

SOX requires public companies to have an **audit committee** of outside, independent directors. The audit committee is responsible for financial reporting, regulatory compliance, internal control, and hiring and overseeing internal and external auditors, who report all critical accounting policies and practices to them.

ORGANIZATIONAL STRUCTURE

A company's organizational structure provides a framework for planning, executing, controlling, and monitoring operations. Important aspects of the organizational structure include the following:

- Centralization or decentralization of authority.
- A direct or matrix reporting relationship.
- Organization by industry, product line, location, or marketing network.
- How allocation of responsibility affects information requirements.
- Organization of and lines of authority for accounting, auditing, and information system functions.
- Size and nature of company activities.

A complex or unclear organizational structure may indicate serious problems. For example, ESM, a brokerage company, used a multilayered organizational structure to hide a $300 million fraud. Management hid stolen cash in their financial statements using a fictitious receivable from a related company.

In today's business world, hierarchical structures, with layers of management who supervise others, are being replaced with flat organizations of self-directed work teams that make decisions without needing multiple layers of approval. The emphasis is on continuous improvement rather than periodic reviews and appraisals. These organizational structure changes impact the nature and type of controls used.

METHODS OF ASSIGNING AUTHORITY AND RESPONSIBILITY

Management should make sure employees understand entity goals and objectives, assign authority and responsibility for goals and objectives to departments and individuals, hold the individuals accountable for achieving them, and encourage the use of initiative to solve problems. It is especially important to identify who is responsible for the company's inforruation security policy.

policy and procedures manual - A document that explains proper business practices, describes needed knowledge and experience, explains document procedures, explains how to handle transactions, and lists the resources provided to carry out specific duties.

Authority and responsibility are assigned and communicated using formal job descriptions, employee training, operating schedules, budgets, a code of conduct, and written policies and procedures. The **policy and procedures manual** explains proper business practices, describes needed knowledge and experience, explains document procedures, explains how to handle transactions, and lists the resources provided to carry out specific duties. The manual

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

includes the chart of accounts and copies of forms and documents. It is a helpful on-the-job reference for current employees and a useful tool for training new employees.

HUMAN RESOURCES STANDARDS THAT ATTRACT, DEVELOP, AND RETAIN COMPETENT INDIVIDUALS

One of the greatest control strengths is the honesty of employees; one of the greatest control weaknesses is the dishonesty of employees. Human resource (HR) policies and practices governing working conditions, job incentives, and career advancement can be a powerful force in encouraging honesty, efficiency, and loyal service. HR policies should convey the required level of expertise, competence, ethical behavior, and integrity required. The following HR policies and procedures are important.

PLAN AND PREPARE FOR SUCCESSION The Board of Directors and management must make plans and prepare for management succession. Top management may need to be replaced at any time for any number of reasons, and an entity should develop a deep management bench—the deeper, the better. While this is most important at the company's highest levels, the company should also plan and prepare for successions in all levels of management as that leads to the desired deep bench of qualified candidates for important management positions.

HIRING Employees should be hired based on educational background, experience, achievements, honesty and integrity, and meeting written job requirements. All company personnel, including cleaning crews and temporary employees, should be subject to hiring policies. Some fraudsters pose as janitors or temporary employees to gain physical access to company computers.

Applicant qualifications can be evaluated using resumes, reference letters, interviews, and background checks. A thorough **background check** includes talking to references, checking for a criminal record, examining credit records, and verifying education and work experience. Many applicants include false information in their applications or resumes. Philip Crosby Associates (PCA) hired John Nelson, MBA, CPA, without conducting a background check. In reality, his CPA designation and glowing references were phony. Nelson was actually Robert W. Liszewski, who had served 18 months in jail for embezzling $400,000. By the time PCA discovered this, Liszewski had embezzled $960,000 using wire transfers to a dummy corporation, supported by forged signatures on contracts and authorization documents.

background check - An investigation of a prospective or current employee that involves verifying their educational and work experience, talking to references, checking for a criminal record or credit problems, and examining other publicly available information.

Many firms hire background check specialists because some applicants buy phony degrees from website operators who "validate" the bogus education when employers call. Some applicants even pay hackers to break into university databases and enter fake graduation or grade data.

COMPENSATING, EVALUATING, AND PROMOTING Poorly compensated employees are more likely to feel resentment and financial pressures that can motivate fraud. Fair pay and appropriate bonus incentives help motivate and reinforce outstanding employee performance. Employees should be given periodic performance appraisals to help them understand their strengths and weaknesses. Promotions should be based on performance and qualifications.

TRAINING Training programs should teach new employees their responsibilities; expected levels of performance and behavior; and the company's policies and procedures, culture, and operating style. Employees can be trained by conducting informal discussions and formal meetings, issuing periodic memos, distributing written guidelines and codes of professional ethics, circulating reports of unethical behavior and its consequences, and promoting security and fraud training programs. Ongoing training helps employees tackle new challenges, stay ahead of the competition, adapt to changing technologies, and deal effectively with the evolving environment.

Fraud is less likely to occur when employees believe security is everyone's business, are proud of their company and protective of its assets, and recognize the need to report fraud. Such a culture has to be created, taught, and practiced. Acceptable and unacceptable behavior should be defined. Many computer professionals see nothing wrong with using corporate computer resources to gain unauthorized access to databases and browse them. The consequences of unethical behavior (reprimands, dismissal, and prosecution) should also be taught and reinforced.

https://fliphtml5.com/pyiue/oxby/basic/301-350 13/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

MANAGING DISGRUNTLED EMPLOYEES Some disgruntled employees, seeking revenge for a perceived wrong, perpetrate fraud or sabotage systems. Companies need procedures to identify disgruntled employees and either help them resolve their feelings or remove them from sensitive jobs. For example, a company may choose to establish grievance channels and provide employee counseling. Helping employees resolve their problems is not easy to do, however, because most employees fear that airing their feelings could have negative consequences.

DISCHARGING Dismissed employees should be removed from sensitive jobs immediately and denied access to the information system. One terminated employee lit a butane lighter under a smoke detector located just outside the computer room. It set off a sprinkler system that ruined most of the computer hardware.

VACATIONS AND ROTATION OF DUTIES Fraud schemes that require ongoing perpetrator attention are uncovered when the perpetrator takes time off. Periodically rotating employee duties and making employees take vacations can achieve the same results. For example, the FBI raided a gambling establishment and discovered that Roswell Steffen, who earned $11,000 a year, was betting $30,000 a day at the racetrack. The bank where he worked discovered that he embezzled and gambled away $1.5 million over a three-year period. A compulsive gambler, Steffen borrowed $5,000 to bet on a "sure thing" that did not pan out. He embezzled ever-increasing amounts in an effort to win back the money he had "borrowed." Steffen's scheme was simple: He transferred money from inactive accounts to his own account. If anyone complained, Steffen, the chief teller with the power to resolve these types of problems, replaced the money by taking it from another inactive account. When asked, after his arrest, how the fraud could have been prevented, Steffen said the bank could have coupled a two-week vacation with several weeks of rotation to another job function. Had the bank taken these measures, Steffen's embezzlement, which required his physical presence at the bank, would have been almost impossible to cover up.

CONFIDENTIALITY AGREEMENTS AND FIDELITY BOND INSURANCE All employees, suppliers, and contractors should sign and abide by a confidentiality agreement. Fidelity bond insurance coverage of key employees protects companies against losses arising from deliberate acts of fraud.

PROSECUTE AND INCARCERATE PERPETRATORS Most fraud is not reported or prosecuted for several reasons:

1. Companies are reluctant to report fraud because it can be a public relations disaster. The disclosure can reveal system vulnerabilities and attract more fraud or hacker attacks.
2. Law enforcement and the courts are busy with violent crimes and have less time and interest for computer crimes in which no physical harm occurs.
3. Fraud is difficult, costly, and time-consuming to investigate and prosecute.
4. Many law enforcement officials, lawyers, and judges lack the computer skills needed to investigate and prosecute computer crimes.
5. Fraud sentences are often light. A famous example involved C. Arnold Smith, former owner of the San Diego Padres, who was named Mr. San Diego of the Century. Smith was involved in the community and made large political contributions. When investigators discovered he had stolen $200 million from his bank, he pleaded no contest. His sentence was four years of probation. He was fined $30,000, to be paid at the rate of $100 a month for 25 years with no interest. Mr. Smith was 71 at the time. The embezzled money was never recovered.

EXTERNAL INFLUENCES

External influences include requirements imposed by stock exchanges, the Financial Accounting Standards Board (FASB), the PCAOB, and the SEC. They also include requirements imposed by regulatory agencies, such as those for banks, utilities, and insurance companies.

https://fliphtml5.com/pyiue/oxby/basic/301-350 14/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

Risk Assessment and Risk Response

Management is responsible for identifying and assessing the threats the company faces. As discussed in Chapter 8, this should include an assessment of all threats, including natural and political disasters, software errors and equipment failures, unintentional acts, and the possibility of intentional acts such as fraud. Considering the risk of fraud is especially important, as it is one of the 17 principles included in the IC framework. Management must identify and analyze risks to determine how they should be managed. They must also identify and assess changes that could significantly impact the system of internal control.

The risks of an identified threat are assessed in several different ways: likelihood, positive and negative impacts, individually and by category, their effect on other organizational units, and on an inherent and a residual basis. **Inherent risk** is the susceptibility of a set of accounts or transactions to significant control problems in the absence of internal control. **Residual risk** is the risk that remains after management implements internal controls or some other response to risk. Companies should assess inherent risk, develop a response, and then assess residual risk.

inherent risk - The susceptibility of a set of accounts or transactions to significant control problems in the absence of internal control.

residual risk - The risk that remains after management implements internal controls or some other response to risk.

To align identified risks with the company's tolerance for risk, management must take an entity-wide view of risk. They must assess a risk's likelihood and impact, as well as the costs and benefits of the alternative responses. Management can respond to risk in one of four ways:

- **Reduce.** Reduce the likelihood and impact of risk by implementing an effective system of internal controls.
- **Accept.** Accept the likelihood and impact of the risk.
- **Share.** Share risk or transfer it to someone else by buying insurance, outsourcing an activity, or entering into hedging transactions.
- **Avoid.** Avoid risk by not engaging in the activity that produces the risk. This may require the company to sell a division, exit a product line, or not expand as anticipated.

Accountants and systems designers help management design effective control systems to reduce inherent risk. They also evaluate internal control systems to ensure that they are operating effectively. They assess and reduce risk using the risk assessment and response strategy shown in Figure 10-3. The first step, threat identification, has already been discussed.

ESTIMATE LIKELIHOOD AND IMPACT

Some threats pose a greater risk because they are more likely to occur. Employees are more likely to make a mistake than to commit fraud, and a company is more likely to be the victim of a fraud than an earthquake. The likelihood of an earthquake may be small, but its impact could destroy a company. The impact of fraud is usually not as great because most instances of fraud do not threaten a company's existence. Likelihood and impact must be considered together. As either increases, both the materiality of the threat and the need to protect against it rise.

Software tools help automate risk assessment and response. Blue Cross Blue Shield of Florida uses ERM software that lets managers enter perceived risks; assess their nature, likelihood, and impact; and assign them a numerical rating. An overall corporate assessment of risk is developed by aggregating all the rankings.

IDENTIFY CONTROLS

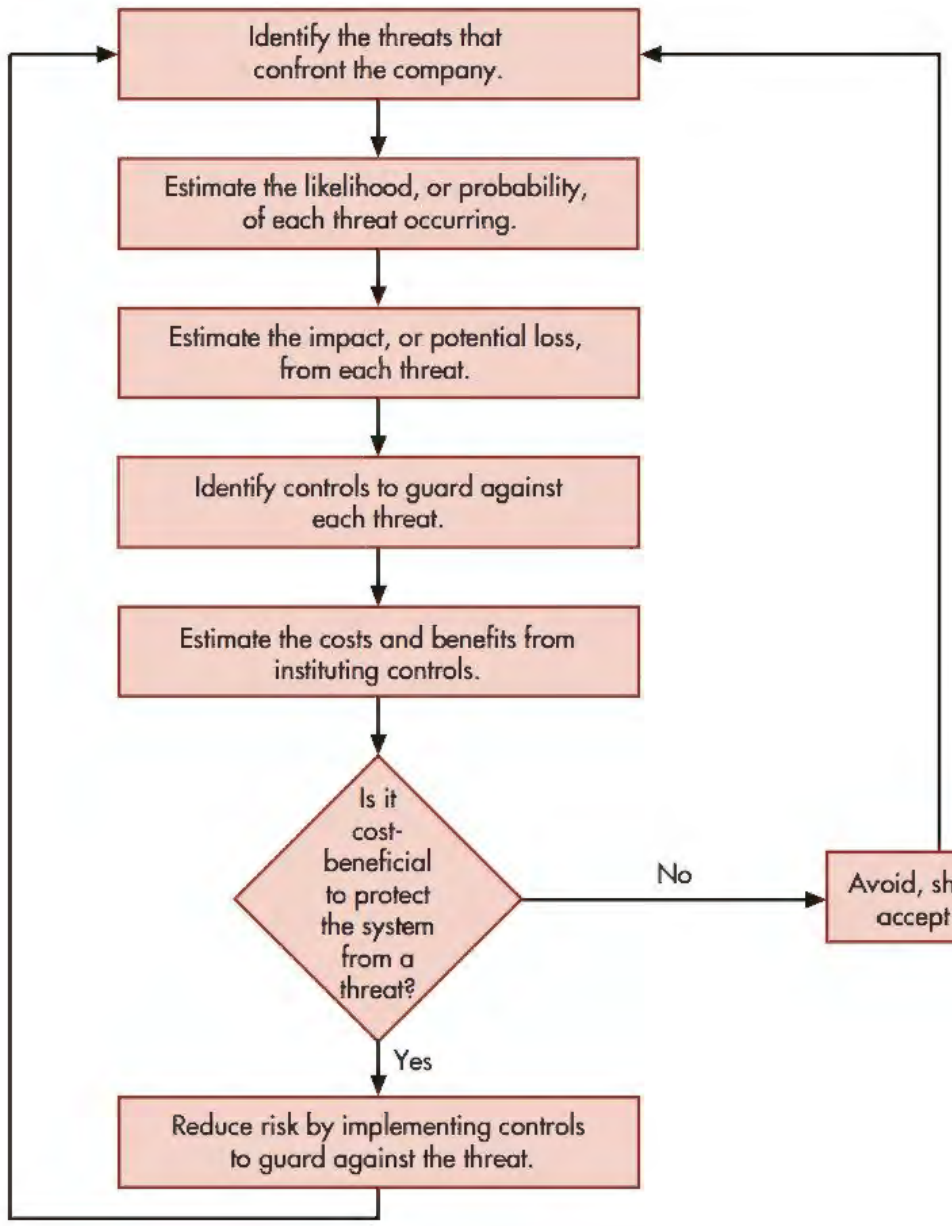
Management should identify controls that protect the company from each threat. Preventive controls are usually superior to detective controls. When preventive controls fail, detective controls are essential for discovering the problem. Corrective controls help recover from any problems. A good internal control system should employ all three.

ESTIMATE COSTS AND BENEFITS

The objective in designing an internal control system is to provide reasonable assurance that threats do not take place. No internal control system provides foolproof protection against all threats because having too many controls is cost-prohibitive and negatively affects operational efficiency. Conversely, having too few controls will not provide the needed reasonable assurance.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

FIGURE 10-3
Risk Assessment Approach to Designing Internal Controls


Identify the threats that confront the company.
Estimate the likelihood, or probability, of each threat occurring.
Estimate the impact, or potential loss, from each threat.
Identify controls to guard against each threat.
Estimate the costs and benefits from instituting controls.
Is it cost-beneficial to protect the system from a threat?
No
Avoid, share, or accept risk.
Yes
Reduce risk by implementing controls to guard against the threat.

The benefits of an internal control procedure must exceed its costs. Benefits, which can be hard to quantify accurately, include increased sales and productivity, reduced losses, better integration with customers and suppliers, increased customer loyalty, competitive advantages, and lower insurance premiums. Costs are usually easier to measure than benefits. A primary cost element is personnel, including the time to perform control procedures, the costs of hiring additional employees to achieve effective segregation of duties, and the costs of programming controls into a computer system.

expected loss - The mathematical product of the potential dollar loss that would occur should a threat become a reality (called *impact* or *exposure*) and the risk or probability that the threat will occur (called *likelihood*).

One way to estimate the value of internal controls involves **expected loss**, the mathematical product of impact and likelihood:

$$\text{Expected loss} = \text{Impact} \times \text{Likelihood}$$

The value of a control procedure is the difference between the expected loss with the control procedure(s) and the expected loss without it.

DETERMINE COST/BENEFIT EFFECTIVENESS

Management should determine whether a control is cost beneficial. For example, at Atlantic Richfield data errors occasionally required an entire payroll to be reprocessed, at a cost of $10,000. A data validation step would reduce the threat likelihood from 15% to 1%, at a cost of $600 per pay period. The cost/benefit analysis that determined that the validation step should be employed is shown in Table 10-2.

In evaluating internal controls, management must consider factors other than those in the expected cost/benefit calculation. For example, if something threatens an organization's existence, its extra cost can be viewed as a catastrophic loss insurance premium.

https://fliphtml5.com/pyiue/oxby/basic/301-350 16/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

TABLE 10-2 Cost/Benefit Analysis of Payroll Validation Procedure

	Without Validation Procedure	With Validation Procedure	Net Expected Difference
Cost to reprocess entire payroll	$10,000	$10,000	
Likelihood of payroll data errors	15%	1%	
Expected reprocessing cost ($10,000 × likelihood)	$1,500	$100	$1,400
Cost of validation procedure	$0	$600	$(600)
Net expected benefit of validation procedure			$800

IMPLEMENT CONTROL OR ACCEPT, SHARE, OR AVOID THE RISK

Cost-effective controls should be implemented to reduce risk. Risks not reduced must be accepted, shared, or avoided. Risk can be accepted if it is within the company's risk tolerance range. An example is a risk with a small likelihood and a small impact. A response to reduce or share risk helps bring residual risk into an acceptable risk tolerance range. A company may choose to avoid the risk when there is no cost-effective way to bring risk into an acceptable risk tolerance range.

Control Activities

Control activities are policies, procedures, and rules that provide reasonable assurance that control objectives are met and risk responses are carried out. It is management's responsibility to develop a secure and adequately controlled system. Management must make sure that:

control activities - Policies, procedures, and rules that provide reasonable assurance that control objectives are met and risk responses are carried out.

1. Controls are selected and developed to help reduce risks to an acceptable level.
2. Appropriate general controls are selected and developed over technology.
3. Control activities are implemented and followed as specified in company policies and procedures.

The information security officer and the operations staff are responsible for ensuring that control procedures are followed.

Controls are much more effective when placed in the system as it is built, rather than as an afterthought. As a result, managers need to involve systems analysts, designers, and end users when designing computer-based control systems. It is important that control activities are in place during the end-of-the-year holiday season because a disproportionate amount of computer fraud and security break-ins takes place during this time. Some reasons for this are (1) extended employee vacations mean that there are fewer people to "mind the store"; (2) students are out of school and have more time on their hands; and (3) lonely counterculture hackers increase their attacks.

Control procedures fall into the following categories:

1. Proper authorization of transactions and activities.
2. Segregation of duties.
3. Project development and acquisition controls.
4. Change management controls.
5. Design and use of documents and records.
6. Safeguarding assets, records, and data.
7. Independent checks on performance.

Focus 10-2 discusses how a violation of specific control activities, combined with control environment factors, resulted in a fraud.

PROPER AUTHORIZATION OF TRANSACTIONS AND ACTIVITIES

Because management lacks the time and resources to supervise each company activity and decision, it establishes policies for employees to follow and then empowers them. This empowerment, called **authorization**, is an important control procedure. Authorizations are

authorization - Establishing policies for employees to follow and then empowering them to perform certain organizational functions. Authorizations are often documented by signing, initializing, or entering an authorization code on a document or record.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

FOCUS 10-2 Control Problems in a School District

The audit report for a school district disclosed serious internal control deficiencies. To improve controls, the district (1) selected a new software package, (2) standardized accounting procedures, (3) instituted purchase order procedures, (4) implemented a separation of duties, and (5) created a control system for vending machine cash and inventory.

After the changes, the director noted that middle school fee balances were low and asked the auditors to investigate. The secretary, responsible for depositing student fees daily and sending them to the central office, said the low amount was due to the principal's waiver of fees for students who qualified for free or reduced-cost lunches. The principal denied having waived the fees.

The auditor examined fee cards for each child and found that the daily deposits did not agree with the dates on student fee cards. They also discovered that the secretary was in charge of a faculty welfare fund that was never audited or examined, nor was it subject to the newly implemented internal controls. Deposits to the fund were checks from the faculty and cash from the vending machines. To perpetrate her $20,000 fraud, the secretary had stolen all the cash from the vending machines, replaced the payee name on vendor checks with her name, and deposited student fees into the faculty welfare fund to cover up the stolen money.

The secretary was immediately discharged. Because the secretary was bonded, the district was able to recover all of its missing funds.

The school district strengthened controls. Internal auditors examine all funds at the schools. Control of faculty welfare funds was transferred to a faculty member. Because the investigation revealed the secretary's prior criminal record, a background check was required for all future hires.

digital signature - A means of electronically signing a document with data that cannot be forged.

specific authorization - Special approval an employee needs in order to be allowed to handle a transaction.

general authorization - The authorization given employees to handle routine transactions without special approval.

often documented by signing, initializing, or entering an authorization code on a document or record. Computer systems can record a **digital signature**, a means of electronically signing a document with data that cannot be forged. Digital signatures are discussed in Chapter 12.

Certain activities or transactions may be of such consequence that management grants **specific authorization** for them to occur. For example, management review and approval may be required for sales in excess of $50,000. In contrast, management can authorize employees to handle routine transactions without special approval, a procedure known as **general authorization**. Management should have written policies on both specific and general authorization for all types of transactions.

Employees who process transactions should verify the presence of appropriate authorizations. Auditors review transactions to verify proper authorization, as their absence indicates a possible control problem. For example, Jason Scott discovered that some purchases did not have a purchase requisition. Instead, they had been "personally authorized" by Bill Springer, the purchasing vice president. Jason also found that some payments had been authorized without proper supporting documents, such as purchase orders and receiving reports. These findings raise questions about the adequacy of Springer's internal control procedures.

SEGREGATION OF DUTIES

Good internal control requires that no single employee be given too much responsibility over business transactions or processes. An employee should not be in a position to commit *and* conceal fraud. Segregation of duties is discussed in two separate sections: segregation of accounting duties and segregation of systems duties.

segregation of accounting duties - Separating the accounting functions of authorization, custody, and recording to minimize an employee's ability to commit fraud.

SEGREGATION OF ACCOUNTING DUTIES As shown in Figure 10-4, effective **segregation of accounting duties** is achieved when the following functions are separated:

- ***Authorization***—approving transactions and decisions.
- ***Recording***—preparing source documents; entering data into computer systems; and maintaining journals, ledgers, files, or databases.
- ***Custody***—handling cash, tools, inventory, or fixed assets; receiving incoming customer checks; writing checks.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

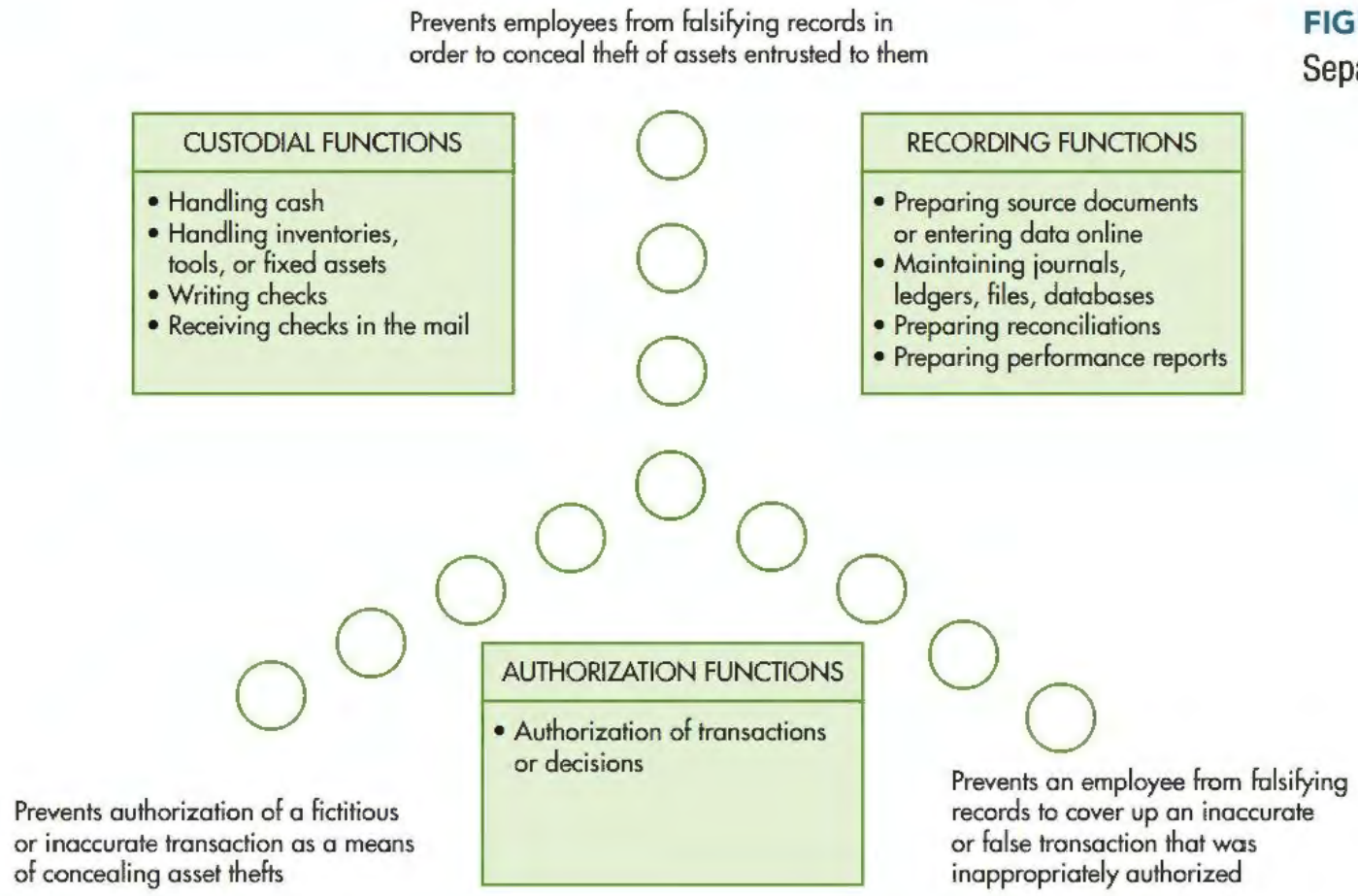

Prevents employees from falsifying records in order to conceal theft of assets entrusted to them
CUSTODIAL FUNCTIONS
• Handling cash
• Handling inventories, tools, or fixed assets
• Writing checks
• Receiving checks in the mail
RECORDING FUNCTIONS
• Preparing source documents or entering data online
• Maintaining journals, ledgers, files, databases
• Preparing reconciliations
• Preparing performance reports
AUTHORIZATION FUNCTIONS
• Authorization of transactions or decisions
Prevents authorization of a fictitious or inaccurate transaction as a means of concealing asset thefts
Prevents an employee from falsifying records to cover up an inaccurate or false transaction that was inappropriately authorized

FIGURE 10-4
Separation of Duties

If one person performs two of these functions, problems can arise. For example, the city treasurer of Fairfax, Virginia, embezzled $600,000. When residents used cash to pay their taxes, she kept the currency and entered the payments on property tax records, but did not report them to the controller. Periodically, she made an adjusting journal entry to bring her records into agreement with those of the controller. When she received checks in the mail that would not be missed if not recorded, she put them in the cash register and stole that amount of cash. Because the treasurer was responsible for both the *custody* of cash receipts and the *recording* of those receipts, she was able to steal cash receipts and falsify the accounts to conceal the theft.

The utilities director of Newport Beach, California, embezzled $1.2 million. Responsible for authorizing transactions, he forged invoices for easement documents authorizing payments to real or fictitious property owners. Finance department officials gave him the checks to deliver to the property owners. He forged signatures and deposited the checks in his own account. Because he was given *custody* of the checks, he could *authorize* fictitious transactions and steal the payments.

The payroll director of the Los Angeles Dodgers embezzled $330,000. He credited employees for hours not worked and received a kickback of 50% of the extra compensation. He added fictitious names to the Dodgers payroll and cashed the paychecks. The fraud was discovered while he was ill and another employee performed his duties. Because the perpetrator was responsible for *authorizing* the hiring of employees and for *recording* employee hours, he did not need to prepare or handle the paychecks. The company mailed the checks to the address he specified.

In a system with effective separation of duties, it is difficult for any single employee to embezzle successfully. Detecting fraud where two or more people are in **collusion** to override controls is more difficult because it is much easier to commit and conceal the fraud. For example, two women at a credit card company colluded. One woman authorized new credit card accounts, and the other wrote off unpaid accounts of less than $1,000. The first woman created a new account for each of them using fictitious data. When the amounts outstanding neared the $1,000 limit, the woman in collections wrote them off. The process would then be repeated. They were caught when a jilted boyfriend seeking revenge reported the scheme to the credit card company.

collusion - Cooperation between two or more people in an effort to thwart internal controls.

Employees can collude with other employees, customers, or vendors. The most frequent employee/vendor collusion includes billing at inflated prices, performing substandard work and receiving full payment, payment for nonperformance, duplicate billings, and improperly purchasing more goods from a colluding company. The most frequent employee/customer collusion

https://fliphtml5.com/pyiue/oxby/basic/301-350 19/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

includes unauthorized loans or insurance payments, receipt of assets or services at unauthorized discount prices, forgiveness of amounts owed, and unauthorized extension of due dates.

SEGREGATION OF SYSTEMS DUTIES In an information system, procedures once performed by separate individuals are sometimes combined. Therefore, any person who has unrestricted access to the computer, its programs, and live data could perpetrate and conceal fraud. To combat this threat, organizations implement **segregation of systems duties**. As shown in Figure 10-5, authority and responsibility should be divided clearly among the seven functions.

segregation of systems duties - Implementing control procedures to clearly divide authority and responsibility within the information system function.

AUTHORIZATION. As explained earlier in the chapter, the proper authorization of transactions and activities is an important control activity. For example, management should:

- Give general authorization to process transactions, such as paying vendors when the goods ordered are received. However, a payment over a certain sum could require specific authorization.
- Approve new business relationships such as a new customer or vendor. If an unapproved vendor was added to the company's database, an employee might be able to make a payment to them as a way of embezzling money. If an unapproved customer was added, sales could be made to a customer with poor credit who is unable to pay.
- Approve all new user account activations to prevent an unauthorized person from having access to company data and business processes.
- Approve the creation or modification of computer programs to prevent unauthorized programs and code.
- Approve the final versions of all new programs and program modifications to ensure they are efficient and do not contain code that harms the organization or that otherwise facilitates unapproved actions.

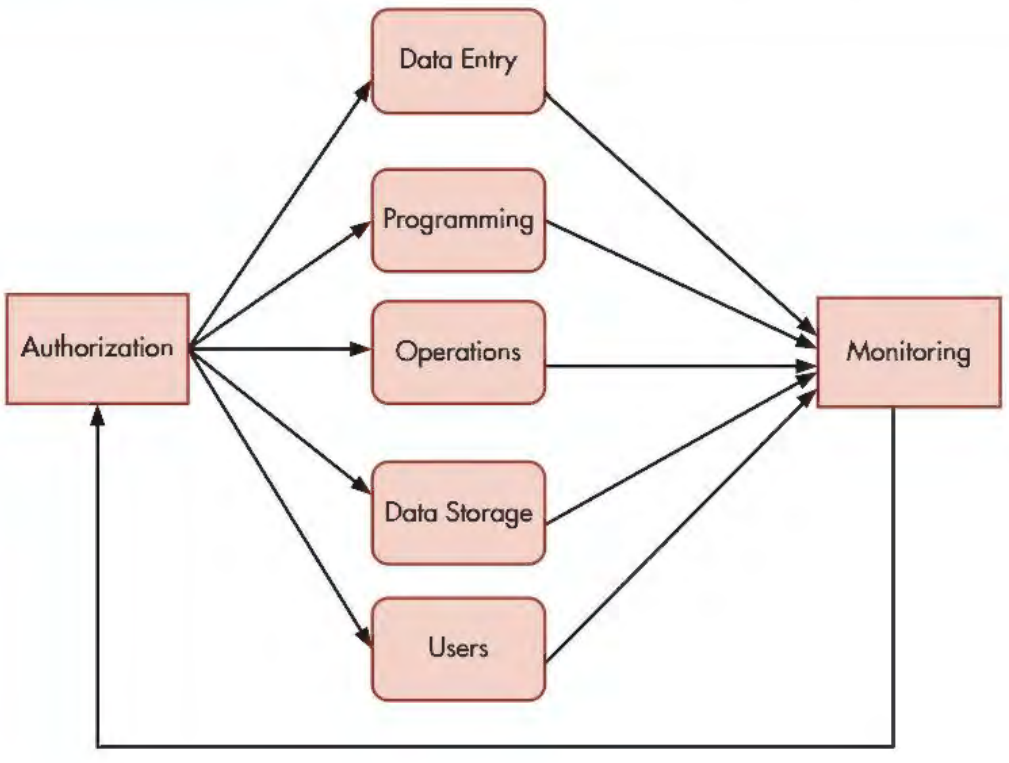
DATA ENTRY. The data entry function is responsible for entering or capturing the data for all business transactions. They are also responsible for the creation of all new user accounts and all new business relationships after their creation has been authorized. Likewise, when authorized to do so, they are responsible for the deletion of no longer needed user accounts and business relationships.

systems analysts - People who help users determine their information needs and design systems to meet those needs.

programmers - People who use the analysts' design to create and test computer programs.

PROGRAMMING. **Systems analysts** help users determine their information needs and design systems to meet those needs. Computer **programmers**, using the system analyst's design, are responsible for developing, coding, and testing all new software applications. They are also responsible for the modification of all existing applications. As explained, they need approval to start the program development or modification activities, and their final products should also be approved.

FIGURE 10-5
Segregation of System Duties



23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

OPERATIONS. **Computer operators** run the software on the company's computers and ensure that data are properly entered, processed correctly, properly stored, and that the needed output is produced. As explained in Chapter 2, transactions can be processed in batch mode (such as periodic payroll) or real time mode (such as airline reservations). Operations may also be responsible for processing approved updates to master accounts such as address changes for customers and vendors).

computer operators - People who operate the company's computers.

DATA STORAGE. The data storage function is responsible for physically storing and maintaining custody of corporate databases, files, and computer programs. They are also responsible for maintaining backup copies of essential company data offsite in a secure location. They maintain physical custody of the IT hardware elements needed for computer operations and processing. Along with users, they are also responsible for safekeeping computer outputs.

USERS. **Users** record transactions, authorize data to be processed, have logical access to company data, and produce system output. They are responsible for safekeeping any data they may access or distribute as system output.

users - People who record transactions, authorize data processing, and use system output.

MANAGEMENT. Top management is responsible for all aspects of a company, including its information system. Since top management have many responsibilities and may not be information system experts, they can employ several different people to help them manage and monitor the AIS. The larger the organization, the more likely top management is to use these people. Some examples of the personnel management teams can use include:

- **Systems administrators** make sure all information system components operate smoothly and efficiently.
- **Network managers** ensure that devices are linked to the organization's internal and external networks and that those networks operate properly.
- **Security management** make sure that systems are secure and protected from internal and external threats.
- **Change management** makes sure changes are made smoothly and efficiently and do not negatively affect systems reliability, security, confidentiality, integrity, and availability.
- **Data control** ensures that source data have been properly approved, monitors the flow of work through the computer, reconciles input and output, maintains a record of input errors to ensure their correction and resubmission, and distributes systems output.
- Database administrators, as described in Chapter 4, are responsible for coordinating, controlling, and managing the database.

systems administrators - People responsible for making sure a system operates smoothly and efficiently.

network managers - People who ensure that the organization's networks operate properly.

security management - People who make sure systems are secure and protected from internal and external threats.

change management - Process of making sure changes are made smoothly and efficiently and do not negatively affect the system.

data control - People who ensure that source data is approved, monitor the flow of work, reconcile input and output, handle input errors, and distribute systems output.

The monitoring function shown in Figure 10-5 is discussed later in the chapter. Allowing a person to perform two or more of the seven functions shown in Figure 10-5 exposes the company to fraud. For example, if a credit union programmer uses actual data to test her program, she could erase her car loan balance during the test. Likewise, if a computer operator has access to programming logic and documentation, he might be able to increase his salary while processing payroll. The key to preventing fraud is to restrict the ability of employees to commit a fraud, conceal it, and convert the fraudulent action into personal gain.

PROJECT DEVELOPMENT AND ACQUISITION CONTROLS

It is important to have a proven methodology to govern the development, acquisition, implementation, and maintenance of information systems. It should contain appropriate controls for management approval, user involvement, analysis, design, testing, implementation, and conversion. These methodologies are discussed in Chapters 22 through 24.

Important systems development controls include the following:

1. A **steering committee** guides and oversees systems development and acquisition.
2. A **strategic master plan** is developed and updated yearly to align an organization's information system with its business strategies. It shows the projects that must be completed, and it addresses the company's hardware, software, personnel, and infrastructure requirements.
3. A **project development plan** shows the tasks to be performed, who will perform them, project costs, completion dates, and **project milestones**—significant points when

steering committee - An executive-level committee to plan and oversee the information systems function.

strategic master plan - A multiple-year plan of the projects the company must complete to achieve its long-range goals.

project development plan - A document that shows how a project will be completed.

project milestones - Points where progress is reviewed and actual and estimated completion times are compared.

https://fliphtml5.com/pyiue/oxby/basic/301-350 21/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

progress is reviewed and actual and estimated completion times are compared. Each project is assigned to a manager and team who are responsible for its success or failure.

4. A **data processing schedule** shows when each task should be performed.
5. **System performance measurements** are established to evaluate the system. Common measurements include **throughput** (output per unit of time), **utilization** (percentage of time the system is used), and **response time** (how long it takes for the system to respond).
6. A **postimplementation review** is performed after a development project is completed to determine whether the anticipated benefits were achieved.

data processing schedule - A schedule that shows when each data processing task should be performed.

system performance measurements - Ways to evaluate and assess a system.

throughput - The amount of work performed by a system during a given period of time.

utilization - The percentage of time a system is used.

response time - How long it takes for a system to respond.

postimplementation review - Review, performed after a new system has been operating for a brief period, to ensure that it meets its planned objectives.

Some companies hire a **systems integrator** to manage a systems development effort involving its own personnel, its client, and other vendors. These development projects are subject to the same cost overruns and missed deadlines as systems developed internally. For example, Westpac Banking began a five-year, $85 million systems development project to decentralize its systems, create new financial products, and downsize its systems department. Three years and $150 million later, no usable results had been attained, and it was clear the scheduled completion date would not be met. With a runaway on its hands, Westpac fired IBM, the primary software developer, and brought in Accenture to review the project and develop recommendations for salvaging it.

systems integrator - An outside party hired to manage a company's systems development effort.

Companies using systems integrators should use the same project management processes and controls as internal projects. In addition, they should:

- **Develop clear specifications.** This includes exact descriptions and system definitions, explicit deadlines, and precise acceptance criteria. Suffolk County, New York, spent 12 months and $500,000 preparing detailed specifications for a $16 million criminal justice system before accepting bids. Only 6 of 22 invited integrators bid on the project because of the county's rigorous cost and quality standards. County officials believe their diligent up-front efforts helped ensure their new system's success and saved the county $3 million.
- **Monitor the project.** Companies should establish formal procedures for measuring and reporting a project's status. The best approach is to divide the project into manageable tasks, assign responsibility for each task, and meet at least monthly to review progress and assess quality.

CHANGE MANAGEMENT CONTROLS

Organizations modify existing systems to reflect new business practices and to take advantage of IT advancements. Those in charge of changes should make sure they do not introduce errors and facilitate fraud. Behavioral aspects of change are discussed in Chapter 22 and change management controls are discussed in Chapter 13.

DESIGN AND USE OF DOCUMENTS AND RECORDS

The proper design and use of electronic and paper documents and records help ensure the accurate and complete recording of all relevant transaction data. Their form and content should be as simple as possible, minimize errors, and facilitate review and verification. Documents that initiate a transaction should contain a space for authorizations. Those that transfer assets need a space for the receiving party's signature. Documents should be sequentially prenumbered so each can be accounted for. An audit trail facilitates tracing individual transactions through the system, correcting errors, and verifying system output. Document, form, and screen design are discussed in Chapter 24.

SAFEGUARD ASSETS, RECORDS, AND DATA

A company must protect its cash and physical assets as well as its information. A reporter for Reuters noticed that Intentia, a Swedish software developer, released its first- and second-quarter earnings reports on websites with nearly identical web addresses. He guessed the third-quarter web address, found their unreleased numbers, and ran a story on the disappointing results. Intentia filed criminal hacking charges, but they were dismissed. The Swedish Stock Exchange censured Intentia for not protecting its financial information.

Employees are a much greater security risk than outsiders are. They are better able to hide their illegal acts because they know system weakness better. Almost 50% of companies report

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

that insiders access data without the proper authorization. A software engineer at America Online was charged with selling 92 million e-mail addresses he illegally obtained using another employee's identity (ID) and password. An Internet gambling business bought the names and used them to increase company earnings by $10,000 to $20,000 a day. The data theft was not uncovered for a year, until an anonymous tipster informed authorities that the gambling business was reselling the names to spammers selling herbal male enhancement products.

Employees also cause unintentional threats, such as accidentally deleting company data, opening virus-laden e-mail attachments, or trying to fix hardware or software without the appropriate expertise. These can result in crashed networks and hardware and software malfunctions as well as corrupt data.

Blockchain can protect data and records as it is tamper-resistant, though not tamper-proof. There are many reasons why it results in a much higher level of transaction integrity. Processed transactions are verified by thousands of networked computers instead of error-prone humans. Duplicate copies of the blockchain are stored on all network computers, eliminating the risks that come with data held centrally. This means there is no single point of failure; if one node goes down, there is a copy of the ledger on the other nodes. Blockchain data is transparent; that is, all transaction details are open for all authorized users to see. Both sides of a transaction are stored in a single source, which can eliminate the need for two sets of books (for the buyer and the seller). One set of books provides a trust level not present in current legacy systems. New blocks are added chronologically to the chain, and blocks are referenced in subsequent blocks. That makes it very difficult to go back and change block contents or add invalid blocks inside the chain because each block contains its own hash and the hash of the previous block. If data is changed or added, the hashes for the previous and subsequent blocks also change, and this disrupts the ledger's shared state. When other network computers become aware that the change has caused a problem, consensus is no longer possible, and future blocks cannot be added until the problem is resolved. Blockchain was introduced in Chapters 1 and 2 and is discussed in more detail in Chapter 12.

Chapters 11 through 13 discuss computer-based controls that help safeguard assets. In addition, it is important to:

- **Create and enforce appropriate policies and procedures.** All too often, policies and procedures are created but not enforced. A laptop with the names, Social Security numbers, and birthdates of 26.5 million people was stolen from the home of a Veteran Affairs (VA) Department analyst. The VA did not enforce its policies that sensitive data be encrypted and not leave VA offices. Notifying all 26.5 million people and buying them a credit-checking service cost taxpayers $100 million. Two years prior to the theft, an inspector general report identified the inadequate control of sensitive data as a weakness, but it had never been addressed.
- **Maintain accurate records of all assets.** Periodically reconcile the recorded amounts of company assets to physical counts of those assets.
- **Restrict access to assets.** Restricting access to storage areas protects inventories and equipment. Cash registers, safes, lockboxes, and safety deposit boxes limit access to cash and paper assets. More than $1 million was embezzled from Perini Corp. because blank checks were kept in an unlocked storeroom. An employee made out checks to fictitious vendors, ran them through an unlocked check-signing machine, and cashed the checks.
- **Protect records and documents.** Fireproof storage areas, locked filing cabinets, backup files, and off-site storage protect records and documents. Access to blank checks and documents should be limited to authorized personnel. In Inglewood, California, a janitor stole 34 blank checks, wrote checks from $50,000 to $470,000, forged the names of city officials, and cashed them.

INDEPENDENT CHECKS ON PERFORMANCE

Independent checks on performance, done by someone other than the person who performs the original operation, help ensure that transactions are processed accurately. They include the following:

- **Top-level reviews.** Management should monitor company results and periodically compare actual company performance to (1) planned performance, as shown in budgets, targets, and forecasts; (2) prior period performance; and (3) competitors' performance.

https://fliphtml5.com/pyiue/oxby/basic/301-350 23/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

analytical review - The examination of the relationships between different sets of data.

- **Analytical reviews.** An **analytical review** is an examination of the relationships between different sets of data. For example, as credit sales increase, so should accounts receivable. In addition, there are relationships between sales and accounts such as cost of goods sold, inventory, and freight out.
- **Reconciliation of independently maintained records.** Records should be reconciled to documents or records with the same balance. For example, a bank reconciliation verifies that company checking account balances agree with bank statement balances. Another example is comparing subsidiary ledger totals with general ledger totals.
- **Comparison of actual quantities with recorded amounts.** Significant assets are periodically counted and reconciled to company records. At the end of each clerk's shift, cash in a cash register drawer should match the amount on the cash register tape. Inventory should be periodically counted and reconciled to inventory records.
- **Double-entry accounting.** The maxim that debits equal credits provides numerous opportunities for independent checks. Debits in a payroll entry may be allocated to numerous inventory and/or expense accounts; credits are allocated to liability accounts for wages payable, taxes withheld, employee insurance, and union dues. After the payroll entries, comparing total debits and credits is a powerful check on the accuracy of both processes. Any discrepancy indicates the presence of an error.
- **Independent review.** After a transaction is processed, a second person reviews the work of the first, checking for proper authorization, reviewing supporting documents, and checking the accuracy of prices, quantities, and extensions.

Communicate Information and Monitor Control Processes

The seventh component in the ERM model is information and communication. The last component is monitoring. Both are discussed in this section of the chapter.

INFORMATION AND COMMUNICATION

Information and communication systems should capture and exchange the information needed to conduct, manage, and control the organization's operations. The primary purpose of an accounting information system (AIS) is to gather, record, process, store, summarize, and communicate information about an organization. This includes understanding how transactions are initiated, data are captured, files are accessed and updated, data are processed, and information is reported. It includes understanding accounting records and procedures, supporting documents, and financial statements. These items provide an **audit trail**, which allows transactions to be traced back and forth between their origination and the financial statements.

audit trail - A path that allows a transaction to be traced through a data processing system from point of origin to output or backward from output to point of origin.

In addition to identifying and recording all valid transactions, an AIS should properly classify transactions, record transactions at their proper monetary value, record transactions in the proper accounting period, and properly present transactions and related disclosures in the financial statements.

Communication must occur internally and externally to provide information needed to carry out day-to-day internal control activities. All personnel must understand their responsibilities.

The updated IC framework specifies that the following three principles apply to the information and communication process:

1. Obtain or generate relevant, high-quality information to support internal control.
2. Internally communicate the information, including objectives and responsibilities, necessary to support the other components of internal control.
3. Communicate relevant internal control matters to external parties.

Accounting systems generally consist of several subsystems, each designed to process a particular type of transaction using the same sequence of procedures, called accounting cycles. The major accounting cycles and their related control objectives and procedures are detailed in Chapters 14 through 18.

https://fliphtml5.com/pyiue/oxby/basic/301-350 24/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

MONITORING

The internal control system that is selected or developed must be continuously monitored, evaluated, and modified as needed. Any deficiencies must be reported to senior management and the board of directors. Key methods of monitoring performance are discussed in this section.

PERFORM INTERNAL CONTROL EVALUATIONS Internal control effectiveness is measured using a formal or a self-assessment evaluation. A team can be formed to conduct the evaluation, or it can be done by internal auditing.

IMPLEMENT EFFECTIVE SUPERVISION Effective supervision involves training and assisting employees, monitoring their performance, correcting errors, and overseeing employees who have access to assets. Supervision is especially important in organizations without responsibility reporting or an adequate segregation of duties.

USE RESPONSIBILITY ACCOUNTING SYSTEMS Responsibility accounting systems include budgets, quotas, schedules, standard costs, and quality standards; reports comparing actual and planned performance; and procedures for investigating and correcting significant variances.

MONITOR SYSTEM ACTIVITIES Risk analysis and management software packages review computer and network security measures, detect illegal access, test for weaknesses and vulnerabilities, report weaknesses found, and suggest improvements. Cost parameters can be entered to balance acceptable levels of risk tolerance and cost-effectiveness. Software also monitors and combats viruses, spyware, adware, spam, phishing, and inappropriate e-mails. It blocks pop-up ads, prevents browsers from being hijacked, and validates a phone caller's ID by comparing the caller's voice to a previously recorded voiceprint. Software can help companies recover from malicious actions. One risk management package helped a company recover from a disgruntled employee's rampage. After a negative performance evaluation, the perpetrator ripped cables out of PCs, changed the inventory control files, and edited the password file to stop people from logging on to the network. The software quickly identified the corrupted files and alerted company headquarters. The damage was undone by utility software, which restored the corrupted file to its original status.

All system transactions and activities should be recorded in a log that indicates who accessed what data, when, and from which online device. These logs should be reviewed frequently and used to monitor system activity, trace problems to their source, evaluate employee productivity, control company costs, fight espionage and hacking attacks, and comply with legal requirements. One company used these logs to analyze why an employee had almost zero productivity and found that he spent six hours a day on porn sites.

The Privacy Foundation estimated that one-third of all American workers with computers are monitored, and that number is expected to increase. Companies who monitor system activities should not violate employee privacy. One way to do that is to have employees agree in writing to written policies that include the following:

- The technology an employee uses on the job belongs to the company.
- E-mails received on company computers are not private and can be read by supervisory personnel. This policy allowed a large pharmaceutical company to identify and terminate an employee who was e-mailing confidential drug-manufacturing data to an external party.
- Employees should not use technology to contribute to a hostile work environment.

TRACK PURCHASED SOFTWARE AND MOBILE DEVICES The Business Software Alliance (BSA) tracks down and fines companies that violate software license agreements. To comply with copyrights and protect themselves from software piracy lawsuits, companies should periodically conduct software audits. There should be enough licenses for all users, and the company should not pay for more licenses than needed. Employees should be informed of the consequences of using unlicensed software.

The increasing number of mobile devices should be tracked and monitored because their loss could represent a substantial exposure. Items to track are the devices, who has them, what tasks they perform, the security features installed, and what software the company needs to maintain adequate system and network security.

https://fliphtml5.com/pyiue/oxby/basic/301-350 25/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

CONDUCT PERIODIC AUDITS External, internal, and network security audits can assess and monitor risk as well as detect fraud and errors. Informing employees of audits helps resolve privacy issues, deters fraud, and reduces errors. Auditors should regularly test system controls and periodically browse system usage files looking for suspicious activities. During the security audit of a health care company, auditors pretending to be computer support staff persuaded 16 of 22 employees to reveal their user IDs and passwords. They also found that employees testing a new system left the company's network exposed to outside attacks.

Internal audits assess the reliability and integrity of financial and operating information, evaluate internal control effectiveness, and assess employee compliance with management policies and procedures as well as applicable laws and regulations. The internal audit function should be organizationally independent of accounting and operating functions. Internal audit should report to the audit committee, not the controller or chief financial officer.

One internal auditor noted that a department supervisor took the office staff to lunch in a limousine on her birthday. Wondering whether her salary could support her lifestyle, he investigated and found she set up several fictitious vendors, sent the company invoices from these vendors, and cashed the checks mailed to her. Over a period of several years, she embezzled more than $12 million.

computer security officer (CSO) - An employee independent of the information system function who monitors the system, disseminates information about improper system uses and their consequences, and reports to top management.

EMPLOY A COMPUTER SECURITY OFFICER AND A CHIEF COMPLIANCE OFFICER A **computer security officer (CSO)** is in charge of system security, independent of the information system function, and reports to the chief operating officer (COO) or the CEO. The overwhelming tasks related to SOX and other forms of compliance have led many companies to delegate all compliance issues to a **chief compliance officer (CCO)**. Many companies use outside computer consultants or in-house teams to test and evaluate security procedures and computer systems.

chief compliance officer (CCO) - An employee responsible for all the compliance tasks associated with SOX and other laws and regulatory rulings.

forensic investigators - Individuals who specialize in fraud, most of whom have specialized training with law enforcement agencies such as the FBI or IRS or have professional certifications such as Certified Fraud Examiner (CFE).

computer forensics specialists - Computer experts who discover, extract, safeguard, and document computer evidence such that its authenticity, accuracy, and integrity will not succumb to legal challenges.

ENGAGE FORENSIC SPECIALISTS **Forensic investigators** who specialize in fraud are a fast-growing group in the accounting profession. Their increasing presence is due to several factors, most notably SOX, new accounting rules, and demands by boards of directors that forensic investigations be an ongoing part of the financial reporting and corporate governance process. Most forensic investigators received specialized training with the FBI, IRS, or other law enforcement agencies. Investigators with the computer skills to ferret out fraud perpetrators are in great demand. The Association of Certified Fraud Examiners sponsors a Certified Fraud Examiner (CFE) professional certification program. To become a CFE, candidates must pass a two-day exam. Currently there are about 35,000 CFEs worldwide.

Computer forensics specialists discover, extract, safeguard, and document computer evidence such that its authenticity, accuracy, and integrity will not succumb to legal challenges. Computer forensics can be compared to performing an "autopsy" on a computer system to determine whether a crime was committed as well as who committed it, and then marshalling the evidence lawyers need to prove the charges in court. Some of the more common matters investigated are improper Internet usage; fraud; sabotage; the loss, theft, or corruption of data; retrieving "erased" information from e-mails and databases; and figuring out who performed certain computer activities. A Deloitte & Touche forensics team uncovered evidence that helped convict a Giant Supermarket purchasing manager who had accepted more than $600,000 in supplier kickbacks.

INSTALL FRAUD DETECTION SOFTWARE Fraudsters follow distinct patterns and leave clues behind that can be discovered by fraud detection software. ReliaStar Financial used software from IBM to detect the following:

- A Los Angeles chiropractor submitted hundreds of thousands of dollars in fraudulent claims. The software identified an unusual number of patients who lived more than 50 miles away from the doctor's office and flagged these bills for investigation.
- A Long Island doctor submitted weekly bills for a rare and expensive procedure normally done only once or twice in a lifetime.
- A podiatrist saw four patients and billed for 500 separate procedures.

neural networks - Computing systems that imitate the brain's learning process by using a network of interconnected processors that perform multiple operations simultaneously and interact dynamically.

Neural networks (programs with learning capabilities) can accurately identify fraud. The Visa and MasterCard operation at Mellon Bank uses a neural network to track 1.2 million

https://fliphtml5.com/pyiue/oxby/basic/301-350 26/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

accounts. It can spot illegal credit card use and notify the owner shortly after the card is stolen. It can also spot trends before bank investigators do. For example, an investigator learned about a new fraud from another bank. When he went to check for the fraud, the neural network had already identified it and had printed out transactions that fit its pattern. The software cost the bank less than $1 million and paid for itself in six months.

IMPLEMENT A FRAUD HOTLINE People witnessing fraudulent behavior are often torn between two conflicting feelings. Although they want to protect company assets and report fraud perpetrators, they are uncomfortable blowing the whistle, so all too often they remain silent. This reluctance is stronger if they are aware of whistle-blowers who have been ostracized, been persecuted, or suffered damage to their careers.

SOX mandates a mechanism for employees to report fraud and abuse. A **fraud hotline** is an effective way to comply with the law and resolve whistle-blower conflict. In one study, researchers found that 33% of 212 frauds were detected through anonymous tips. The insurance industry set up a hotline to control $17 billion a year in fraudulent claims. In the first month, more than 2,250 calls were received; 15% resulted in investigative action. The downside of hotlines is that many calls are not worthy of investigation; some are motivated by a desire for revenge, some are vague reports of wrongdoing, and others have no merit.

fraud hotline - A phone number employees can call to anonymously report fraud and abuse.

Summary and Case Conclusion

One week after Jason and Maria filed their audit report, they were summoned to the office of Northwest's director of internal auditing to explain their findings. Shortly thereafter, a fraud investigation team was dispatched to Bozeman to take a closer look at the situation. Six months later, a company newsletter indicated that the Springer family sold its 10% interest in the business and resigned from all management positions. Two Northwest executives were transferred in to replace them. There was no other word on the audit findings.

Two years later, Jason and Maria worked with Frank Ratliff, a member of the high-level audit team. After hours, Frank told them the investigation team examined a large sample of purchasing transactions and all employee timekeeping and payroll records for a 12-month period. The team also took a detailed physical inventory. They discovered that the problems Jason identified—including missing purchase requisitions, purchase orders, and receiving reports, as well as excessive prices—were widespread. These problems occurred in transactions with three large vendors from whom Springer's had purchased several million dollars of inventory. The investigators discussed the unusually high prices with the vendors but did not receive a satisfactory explanation. The county business-licensing bureau revealed that Bill Springer held a majority ownership interest in each of these companies. By authorizing excessive prices to companies he owned, Springer earned a significant share of several hundred thousand dollars of excessive profits, all at the expense of Northwest Industries.

Several Springer employees were paid for more hours than they worked. Inventory was materially overstated; a physical inventory revealed that a significant portion of recorded inventory did not exist and that some items were obsolete. The adjusting journal entry reflecting Springer's real inventory wiped out much of their profits over the past three years.

When confronted, the Springers vehemently denied breaking any laws. Northwest considered going to the authorities but was concerned that the case was not strong enough to prove in court. Northwest also worried that adverse publicity might damage the company's position in Bozeman. After months of negotiation, the Springers agreed to the settlement reported in the newsletter. Part of the settlement was that no public statement would be made about any alleged fraud or embezzlement involving the Springers. According to Frank, this policy was normal. In many fraud cases, settlements are reached quietly, with no legal action taken, so that the company can avoid adverse publicity.

https://fliphtml5.com/pyiue/oxby/basic/301-350 27/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

KEY TERMS

threat 324
exposure/impact 324
likelihood/risk 324
internal controls 324
preventive controls 324
detective controls 324
corrective controls 324
general controls 324
application controls 324
belief system 325
boundary system 325
diagnostic control system 325
interactive control system 325
Foreign Corrupt Practices Act (FCPA) 325
Sarbanes–Oxley Act (SOX) 325
Public Company Accounting Oversight Board (PCAOB) 325
Control Objectives for Information and Related Technology (COBIT) 326
Committee of Sponsoring Organizations (COSO) 328
Internal Control—Integrated Framework (IC) 328
control environment 330
risk appetite 331
audit committee 332
policy and procedures manual 332
background check 333
inherent risk 335
residual risk 335
expected loss 336
control activities 337
authorization 337
digital signature 338
specific authorization 338
general authorization 338
segregation of accounting duties 338
collusion 339
segregation of systems duties 340
systems analysts 340
programmers 340
computer operators 341
users 341
systems administrators 341
network managers 341
security management 341
change management 341
data control 341
steering committee 341
strategic master plan 341
project development plan 341
project milestones 341
data processing schedule 342
system performance measurements 342
throughput 342
utilization 342
response time 342
postimplementation review 342
systems integrator 342
analytical review 344
audit trail 344
computer security officer (CSO) 346
chief compliance officer (CCO) 346
forensic investigators 346
computer forensics specialists 346
neural networks 346
fraud hotline 347

AIS in Action

CHAPTER QUIZ

1. Verifying the validity of credit or debit card numbers during an online transaction is an example of
   a. detective controls.
   b. preventive controls.
   c. application controls.
   d. general controls.

2. Which one of the following is a key principle of the COBIT 5 framework?
   a. ensuring an approach where governance is effectively managed
   b. focusing on IT operations
   c. distinguishing between governance and management
   d. aligning with other standards at a low level to create a support framework for IT governance and management

3. Which of the following statements is true?
   a. COSO's internal control integrated framework is used to clearly define internal controls, but the evaluation of the control systems is handled elsewhere.
   b. Control activities in COSO's internal control model focus on control activities that are performed at the management level.
   c. The ERM model developed by COSO has a rigid three-dimensional structure that addresses four fixed management objectives, eight interrelated risk and control elements, and five subunits within each company.
   d. The ERM framework is much more comprehensive than the widely adopted IC framework.

https://fliphtml5.com/pyiue/oxby/basic/301-350 28/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

4. All other things being equal, which of the following is true?
   a. Detective controls are superior to preventive controls.
   b. Corrective controls are superior to preventive controls.
   c. Preventive controls are equivalent to detective controls.
   d. Preventive controls are superior to detective controls.

5. Which of the following should assist management in reconciling the conflict between creativity and control?
   a. measuring and monitoring actual company progress with the help of a boundary system
   b. using a belief system that describes how a company creates value, assists employees to understand management's vision, and inspires employees to live by those core company values
   c. encouraging employees to attempt to act ethically by establishing boundaries on employee behavior so as to creatively solve problems
   d. focusing subordinates' attention on key operational issues through interactive control systems and not interfering in their decisions

6. To achieve effective segregation of duties, certain functions must be separated. Which of the following is the correct listing of the accounting-related functions that must be segregated?
   a. control, recording, and monitoring
   b. authorization, recording, and custody
   c. control, custody, and authorization
   d. monitoring, recording, and planning

7. Which of the following is not an independent check?
   a. bank reconciliation
   b. periodic comparison of subsidiary ledger totals to control accounts
   c. trial balance
   d. re-adding the total of a batch of invoices and comparing it with your first total

8. Which of the following is a control procedure relating to both the design and the use of documents and records?
   a. locking blank checks in a drawer
   b. reconciling the bank account
   c. sequentially prenumbering sales invoices
   d. comparing actual physical quantities with recorded amounts

9. Which of the following is the correct order of the risk assessment steps discussed in this chapter?
   a. identify threats, estimate risk and exposure, identify controls, estimate costs and benefits
   b. identify controls, estimate risk and exposure, identify threats, estimate costs and benefits
   c. estimate risk and exposure, identify controls, identify threats, estimate costs and benefits
   d. estimate costs and benefits, identify threats, identify controls, estimate risk and exposure

10. Your company's current system is 85% reliable. A major threat has been identified with an impact of €7,500,000. Two possible control procedures can be implemented to deal with the identified threat. Implementation of control A would cost €45,000 and reduce the likelihood to 7%. Implementation of control B would cost €40,000 and reduce the likelihood to 4%. Implementation of both controls would cost €70,000 and reduce the likelihood to 3%. Given this information, and based solely on an economic analysis of cost and benefits, what should you do?
   a. Implement control A only.
   b. Implement control B only.
   c. Implement both controls A and B.
   d. Implement neither control.

DISCUSSION QUESTIONS

10.1 Answer the following questions about the audit of Springer's Lumber & Supply.
   a. What deficiencies existed in the control environment at Springer's?
   b. Do you agree with the decision to settle with the Springers rather than to prosecute them for fraud and embezzlement? Why, or why not?
   c. Should the company have told Jason and Maria the results of the high-level audit? Why, or why not?

https://fliphtml5.com/pyiue/oxby/basic/301-350 29/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

10.2 Explain why the Foreign Corrupt Practices Act was important to accountants.

10.3 One function of the AIS is to provide adequate controls to ensure the safety of organizational assets, including data. However, many people view control procedures as "red tape." They also believe that instead of producing tangible benefits, business controls create resentment and loss of company morale. Discuss this position.

10.4 In recent years, Supersmurf's external auditors have given clean opinions on its financial statements and favorable evaluations of its internal control systems. Discuss whether it is necessary for this corporation to take any further action to comply with the Sarbanes–Oxley Act.

10.5 When you go to a movie theater, you buy a prenumbered ticket from the cashier. This ticket is handed to another person at the entrance to the movie. What kinds of irregularities is the theater trying to prevent? What controls is it using to prevent these irregularities? What remaining risks or exposures can you identify?

10.6 Some restaurants use customer checks with prenumbered sequence codes. Each food server uses these checks to write up customer orders. Food servers are told not to destroy any customer checks; if a mistake is made, they are to void that check and write a new one. All voided checks are to be turned in to the manager daily. How does this policy help the restaurant control cash receipts?

10.7 Discuss the weaknesses in COSO's internal control framework that led to the development of the COSO Enterprise Risk Management framework.

PROBLEMS

10.1 You are an audit supervisor assigned to a new client, Go-Go Corporation, which is listed on the New York Stock Exchange. You visited Go-Go's corporate headquarters to become acquainted with key personnel and to conduct a preliminary review of the company's accounting policies, controls, and systems. During this visit, the following events occurred:

a. You met with Go-Go's audit committee, which consists of the corporate controller, treasurer, financial vice president, and budget director.
b. You recognized the treasurer as a former aide to Ernie Eggers, who was convicted of fraud several years ago.
c. Management explained its plans to change accounting methods for depreciation from the accelerated to the straight-line method. Management implied that if your firm does not concur with this change, Go-Go will employ other auditors.
d. You learned that the financial vice president manages a staff of five internal auditors.
e. You noted that all management authority seems to reside with three brothers, who serve as chief executive officer, president, and financial vice president.
f. You were told that the performance of division and department managers is evaluated on a subjective basis because Go-Go's management believes that formal performance evaluation procedures are counterproductive.
g. You learned that the company has reported increases in earnings per share for each of the past 25 quarters; however, earnings during the current quarter have leveled off and may decline.
h. You reviewed the company's policy and procedures manual, which listed policies for dealing with customers, vendors, and employees.
i. Your preliminary assessment is that the accounting systems are well designed and that they employ effective internal control procedures.
j. Some employees complained that some managers occasionally contradict the instructions of other managers regarding proper data security procedures.
k. After a careful review of the budget for data security enhancement projects, you feel the budget appears to be adequate.
l. The enhanced network firewall project appeared to be on a very aggressive implementation schedule. The IT manager mentioned that even if he put all of his personnel on the project for the next five weeks, he still would not complete the project

https://fliphtml5.com/pyiue/oxby/basic/301-350 30/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

in time. The manager has mentioned this to company management, which seems unwilling to modify the schedule.

m. Several new employees have had trouble completing some of their duties, and they do not appear to know who to ask for help.

n. Go-Go's strategy is to achieve consistent growth for its shareholders. However, its policy is not to invest in any project unless its payback period is no more than 48 months and yields an internal rate of return that exceeds its cost of capital by 3%.

o. You observe that company purchasing agents wear clothing and exhibit other paraphernalia from major vendors. The purchasing department manager proudly displays a picture of himself holding a big fish on the deck of a luxury fishing boat that has the logo of a major Go-Go vendor painted on its wheelhouse.

REQUIRED

The information you have obtained suggests potential problems relating to Go-Go's control environment. Identify the problems, and explain them in relation to the control environment concepts discussed in this chapter.

10.2 Explain how independent performance evaluation procedures are either violated or effectively applied in each of the following situations. Identify the problem and suggest the check required (or applied) to prevent the identified problem from occurring.

a. The manager who oversees the corporate fleet vehicles signed off on the purchase of 15 luxury SUVs to expand the company's fleet of cars. As soon as this was done, he instructed that the payment be made.

b. At a newly opened local restaurant, waiters work six-hour shifts. There are three six-hour shifts per day, with each shift overlapping the next. The restaurant currently has two cash registers and these can be operated by any one of the waiters during a shift without them requiring any form of identification. The new manager has decided that the cash in the cash register box will be checked once every 24 hours, i.e., in the mornings before the new shift for the day begins.

c. A company's financial clerk does a spot check of the account books and finds that there is a discrepancy between the balances of the checking account and the bank statement.

d. In July of the previous year, the inventory clerk suspects that the warehouse inventory level is not being reflected accurately. When the year-end inventory was reviewed at the end of February of this year, his suspicions were confirmed.

e. There was a spike in credit sales that was not picked up by the credit sales controller. When he was confronted by his line manager about it, he blamed the accounts receivable department for not identifying the issue earlier. The accounts receivable department denies that there was a spike in credit sales as their records do not indicate such a change.

f. A new employee at a company identifies a discrepancy between the total debits and total credits after payroll entries were finalized.

g. A client calls up a store to check the availability of a specific product at the store. The client is informed by the sales manager that he has checked their inventory system and the stock is available for the specific product. The customer visits the store, only to find that the product is no longer in stock. Upon querying the cashier, the client is again informed that the inventory system shows a relatively large quantity of the product stock being available. However, no one at the store is able to locate this stock.

h. Over a period of five years, one of the managers in a company realizes that the company does not seem to be performing as well as it forecasts and budgets for. However, he optimistically goes on believing that things will turn for the better.

i. In order to speed up the processing of sales transactions, one person was made responsible both for the sales journal as well as the accounts receivable master file.

j. The supervisor at a local hypermarket verifies the accuracy of the cash in the cash register box assigned to a retail clerk. Every so often an internal auditor verifies if the supervisor actually performed this check.

k. The payroll clerk realizes that the time sheets and absence records of a specific department in the organization were not in line with company policy. The supervisor of this specific department has been on sick leave for the last three months.

https://fliphtml5.com/pyiue/oxby/basic/301-350 31/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

10.3 Match the terms with their definitions:

____	**1.** inherent risk	a.	Outside party hired to manage systems development effort
____	**2.** general authorization	b.	Probability that a threat will come to pass
____	**3.** control environment	c.	Risk that remains after management implements internal controls or some other response to risk
____	**4.** corrective controls	d.	Cooperation between two or more people to thwart internal controls
____	**5.** risk appetite	e.	Special approval needed to handle a transaction.
____	**6.** application controls	f.	Company culture that is the foundation for all other internal control components
____	**7.** systems integrator	g.	Person who ensures an organization's networks operate properly
____	**8.** utilization	h.	Ensures source data is approved, monitors work flow, and handles input errors
____	**9.** security management	i.	Susceptibility of accounts or transactions to control problems in absence of internal control
____	**10.** strategic master plan	j.	Path used to trace a transaction from origin to output or from output to origin
____	**11.** specific authorization	k.	Amount of work performed during a given time period
____	**12.** collusion	l.	Electronically signing a document with data that cannot be forged
____	**13.** throughput	m.	Controls that prevent, detect, and correct transaction errors and fraud in transaction processing programs
____	**14.** systems administrator	n.	Given to employees to handle routine transactions without special approval
____	**15.** residual risk	o.	Controls that identify and correct problems and recover from resulting errors
____	**16.** data control	p.	Responsible for making sure a system operates smoothly and efficiently
____	**17.** likelihood	q.	Document that shows how a project will be completed
____	**18.** analytical review	r.	Amount of risk company is willing to accept to achieve its goals and objectives
____	**19.** exposure	s.	Makes sure systems are secure and protected from internal and external threats
____	**20.** systems analysts	t.	Percentage of time a system is used
____	**21.** audit trail	u.	Examining relationships between different sets of data
____	**22.** audit committee	v.	Potential dollar loss if a threat becomes a reality
____	**23.** digital signature	w.	Outside, independent directors responsible for financial reporting, regulatory compliance, and internal control
		x.	Controls designed to discover control problems not prevented
		y.	Multiple year plan of projects company must complete to achieve long-range goals
		z.	Help users determine their information needs and design systems to meet those needs

https://fliphtml5.com/pyiue/oxby/basic/301-350 32/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

10.4 The Garden Nursery, a client of your firm, has come to you with the following problem. It has three clerical employees who must perform the following functions:

a. Approve vendor selection
b. Maintain vendor payment terms
c. Maintain accounts payable ledger
d. Handle inventory received
e. Authorize purchase orders
f. Approve receiving reports
g. Maintain vendor records
h. Authorize cash disbursement

Assuming equal abilities among the three employees, the company asks you to assign the eight functions to them to maximize internal control. Assume that these employees will perform no accounting functions other than the ones listed.

REQUIRED

a. List four possibly unsatisfactory pairings of the functions.
b. State how you would distribute the functions among the three employees. Assume that all functions require an equal amount of time to be completed.

10.5 During a recent review, ABC Corporation discovered that it has a serious internal control problem. It is estimated that the impact associated with this problem is $1 million and that the likelihood is currently 5%. Two internal control procedures have been proposed to deal with this problem. Procedure A would cost $25,000 and reduce likelihood to 2%; procedure B would cost $30,000 and reduce likelihood to 1%. If both procedures were implemented, likelihood would be reduced to 0.1%.

REQUIRED

a. What is the estimated expected loss associated with ABC Corporation's internal control problem before any new internal control procedures are implemented?
b. Compute the revised estimate of expected loss if procedure A were implemented, if procedure B were implemented, and if both procedures were implemented.
c. Compare the estimated costs and benefits of procedure A, procedure B, and both procedures combined. If you consider only the estimates of cost and benefit, which procedure(s) should be implemented?
d. What other factors might be relevant to the decision?
e. Use the Goal Seek function in Microsoft Excel to determine the likelihood of occurrence without the control and the reduction in expected loss if the net benefit/cost is 0. Do this for procedure A, procedure B, and both procedures together.

10.6 The management at MechDesign Industries recognizes that a well-designed internal control system provides many benefits. Among the benefits are reliable financial records that support decision making and a greater probability of detecting errors and preventing fraud. MechDesign Industries' internal auditing department periodically reviews the company's accounting records to determine the effectiveness of internal controls. In its latest review, the internal audit staff found the following eight conditions:

1. Many purchases were personally approved by the purchasing department manager and did not have a corresponding purchase requisition.
2. The prices of some raw materials purchased from a specific vendor are unusually high and this vendor is not on the preferred vendor list.
3. There was a sudden increase in backorders for recorded sales orders over the last two months.
4. Many purchase orders are recorded as being open. However, when the purchase order tracking is done, orders have been received.
5. There are many customers returns due to defective products.
6. Since cleaning materials are not part of the production stock, and the maintenance supervisor is responsible for the cleaning materials' requisitioning, he also orders and receives the cleaning materials.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

7. Many employees have access to a range of business processes and activities—including to some of the functions that they do not currently perform.
8. The payroll director has been working in the company for about six years without taking a single day of leave. When the employee was unexpectedly hospitalized, fictitious employees were identified on the payroll by the director who had temporarily replaced the hospitalized employee.

REQUIRED

For each of the eight conditions detected by the company's internal audit staff:

a. Identify a possible cause of the condition.
b. Recommend controls and/or actions would correct the condition and prevent it from happening again.

10.7 For the following scenarios, describe the recommendations the internal auditors should make to prevent these problems in the future.

Scenario 1: After working together at a local school cafeteria for over eight years, two elderly women employees announce their retirement citing reasons of wanting to spend more time with their families. They were loved by the learners at the school and were considered to be considerate, pleasant, caring, and loyal by the other employees at the cafeteria as well as the school authorities. They also always offered to come in early to work and stay back late to cash up. However, soon after their retirement, the authorities discover a sharp increase in their daily cash deposits for the cafeteria. Noting this significant difference, they investigated the matter, and the retired employees' theft was uncovered.

Scenario 2: An employee who works in the production department of a large company manages to get access to the company storehouse. He pockets several materials from the storehouse, only some of which was purchased for his personal use. In the inventory journal, he excludes the quantity purchased for his personal use in recording the parts issued to the production department. Noting differences in the inventory records and the actual quantities available at the storehouse, the company hires an internal auditor to investigate the matter.

10.8 Tralor Corporation manufactures and sells several different lines of small electric components. Its internal audit department completed an audit of its expenditure processes. Part of the audit involved a review of the internal accounting controls for payables, including the controls over the authorization of transactions, accounting for transactions, and the protection of assets. The auditors noted the following items:

1. Routine purchases are initiated by inventory control notifying the purchasing department of the need to buy goods. The purchasing department fills out a prenumbered purchase order and gets it approved by the purchasing manager. The original of the five-part purchase order goes to the vendor. The other four copies are for purchasing, the user department, receiving for use as a receiving report, and accounts payable.
2. For efficiency and effectiveness, purchases of specialized goods and services are negotiated directly between the user department and the vendor. Company procedures require that the user department and the purchasing department approve invoices for any specialized goods and services before making payment.
3. Accounts payable maintains a list of employees who have purchase order approval authority. The list was updated two years ago and is seldom used by accounts payable clerks.
4. Prenumbered vendor invoices are recorded in an invoice register that indicates the receipt date, whether it is a special order, when a special order is sent to the requesting department for approval, and when it is returned. A review of the register indicated that there were seven open invoices for special purchases, which had been forwarded to operating departments for approval over 30 days previously and had not yet been returned.
5. Prior to making entries in accounting records, the accounts payable clerk checks the mathematical accuracy of the transaction, makes sure all transactions are properly documented (the purchase order matches the signed receiving report and the vendor's invoice), and obtains departmental approval for special purchase invoices.
6. All approved invoices are filed alphabetically. Invoices are paid on the 5th and 20th of each month, and all cash discounts are taken regardless of the terms.

https://fliphtml5.com/pyiue/oxby/basic/301-350 34/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

7. The treasurer signs the checks and cancels the supporting documents. An original document is required for a payment to be processed.
8. Prenumbered blank checks are kept in a locked safe accessible only to the cash disbursements department. Other documents and records maintained by the accounts payable section are readily accessible to all persons assigned to the section and to others in the accounting function.

REQUIRED

Review the eight items listed, and decide whether they represent an internal control strength or weakness.

a. For each internal control strength you identified, explain how the procedure helps achieve good authorization, accounting, or asset protection control.
b. For each internal control weakness you identified, explain why it is a weakness and recommend a way to correct the weakness. (*CMA, adapted*)

10.9 Lancaster Company makes electrical parts for contractors and home improvement retail stores. After their annual audit, Lancaster's auditors commented on the following items regarding internal controls over equipment:

1. The operations department that needs the equipment normally initiates a purchase requisition for equipment. The operations department supervisor discusses the proposed purchase with the plant manager. If there are sufficient funds in the requesting department's equipment budget, a purchase requisition is submitted to the purchasing department once the plant manager is satisfied that the request is reasonable.
2. When the purchasing department receives either an inventory or an equipment purchase requisition, the purchasing agent selects an appropriate supplier and sends them a purchase order.
3. When equipment arrives, the user department installs it. The property, plant, and equipment control accounts are supported by schedules organized by year of acquisition. The schedules are used to record depreciation using standard rates, depreciation methods, and salvage values for each type of fixed asset. These rates, methods, and salvage values were set 10 years ago during the company's initial year of operation.
4. When equipment is retired, the plant manager notifies the accounting department so the appropriate accounting entries can be made.
5. There has been no reconciliation since the company began operations between the accounting records and the equipment on hand.

REQUIRED

Identify the internal control weaknesses in Lancaster's system, and recommend ways to correct them. (*CMA, adapted*)

10.10 The Langston Recreational Company (LRC) manufactures ice skates for racing, figure skating, and hockey. The company is in Kearns, Utah, so it can be close to the Olympic Ice Shield, where many Olympic speed skaters train.

Given the precision required to make skates, tracking manufacturing costs is very important to management so it can price the skates appropriately. To capture and collect manufacturing costs, the company acquired an automated cost accounting system from a national vendor. The vendor provides support, maintenance, and data and program backup service for LRC's system.

LRC operates one shift, five days a week. All manufacturing data are collected and recorded by Saturday evening so that the prior week's production data can be processed. One of management's primary concerns is how the actual manufacturing process costs compare with planned or standard manufacturing process costs. As a result, the cost accounting system produces a report that compares actual costs with standard costs and provides the difference, or variance. Management focuses on significant variances as one means of controlling the manufacturing processes and calculating bonuses.

Occasionally, errors occur in processing a week's production cost data, which requires the entire week's cost data to be reprocessed at a cost of $34,500. The current risk of error without any control procedures is 8%. LRC's management is currently considering a set of cost accounting control procedures that is estimated to reduce the

https://fliphtml5.com/pyiue/oxby/basic/301-350 35/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

risk of the data errors from 8% to 3%. This data validation control procedure is projected to cost $1,000 per week.

REQUIRED

a. Perform a cost/benefit analysis of the data validation control procedures.
b. Based on your analysis, make a recommendation to management regarding the control procedure.
c. The current risk of data errors without any control procedures is estimated to be 8%. The data control validation procedure costs $1,000 and reduces the risk to 3%. At some point between 8% and 3% is a point of indifference—that is, Cost of reprocessing the data without controls = Cost of processing the data with the controls + Cost of controls. Use a spreadsheet application such as Excel Goal Seek to find the solution.

CASE 10-1 The Greater Providence Deposit & Trust Embezzlement

Nino Moscardi, president of Greater Providence Deposit & Trust (GPD&T), received an anonymous note in his mail stating that a bank employee was making bogus loans. Moscardi asked the bank's internal auditors to investigate the transactions detailed in the note. The investigation led to James Guisti, manager of a North Providence branch office and a trusted 14-year employee who had once worked as one of the bank's internal auditors. Guisti was charged with embezzling $1.83 million from the bank using 67 phony loans taken out over a three-year period.

Court documents revealed that the bogus loans were 90-day notes requiring no collateral and ranging in amount from $10,000 to $63,500. Guisti originated the loans; when each one matured, he would take out a new loan, or rewrite the old one, to pay the principal and interest due. Some loans had been rewritten five or six times.

The 67 loans were taken out by Guisti in five names, including his wife's maiden name, his father's name, and the names of two friends. These people denied receiving stolen funds or knowing anything about the embezzlement. The fifth name was James Vanesse, who police said did not exist. The Social Security number on Vanesse's loan application was issued to a female, and the phone number belonged to a North Providence auto dealer.

Lucy Fraioli, a customer service representative who cosigned the checks, said Guisti was her supervisor and she thought nothing was wrong with the checks, though she did not know any of the people. Marcia Perfetto, head teller, told police she cashed checks for Guisti made out to four of the five persons. Asked whether she gave the money to Guisti when he gave her checks to cash, she answered, "Not all of the time," though she could not recall ever having given the money directly to any of the four, whom she did not know.

Guisti was authorized to make consumer loans up to a certain dollar limit without loan committee approvals, which is a standard industry practice. Guisti's original lending limit was $10,000, the amount of his first fraudulent loan. The dollar limit was later increased to $15,000 and then increased again to $25,000. Some of the loans, including the one for $63,500, far exceeded his lending limit. In addition, all loan applications should have been accompanied by the applicant's credit history report, purchased from an independent credit rating firm. The loan taken out in the fictitious name would not have had a credit report and should have been flagged by a loan review clerk at the bank's headquarters.

News reports raised questions about why the fraud was not detected earlier. State regulators and the bank's internal auditors failed to detect the fraud. Several reasons were given for the failure to find the fraud earlier. First, in checking for bad loans, bank auditors do not examine all loans and generally focus on loans much larger than the ones in question. Second, Greater Providence had recently dropped its computer services arrangement with a local bank in favor of an out-of-state bank. This changeover may have reduced the effectiveness of the bank's control procedures. Third, the bank's loan review clerks were rotated frequently, making follow-up on questionable loans more difficult.

Guisti was a frequent gambler and used the embezzled money to pay gambling debts. The bank's losses totaled $624,000, which was less than the $1.83 million in bogus loans because Guisti used a portion of the borrowed money to repay loans as they came due. The bank's bonding company covered the loss.

The bank experienced other adverse publicity prior to the fraud's discovery. First, the bank was fined $50,000 after pleading guilty to failure to report cash transactions exceeding $10,000, which is a felony. Second, bank owners took the bank private after a lengthy public battle with the State Attorney General, who alleged that the bank inflated its assets and overestimated its capital surplus to make its balance sheet look stronger. The bank denied this charge.

1. How did Guisti commit the fraud, conceal it, and convert the fraudulent actions to personal gain?

https://fliphtml5.com/pyiue/oxby/basic/301-350 36/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

2. Good internal controls require that the custody, recording, and authorization functions be separated. Explain which of those functions Guisti had and how the failure to segregate them facilitated the fraud.
3. Identify the preventive, detective, and corrective controls at GPD&T, and discuss whether they were effective.
4. Explain the pressures, opportunities, and rationalizations that were present in the Guisti fraud.
5. Discuss how Greater Providence Deposit & Trust might improve its control procedures over the disbursement of loan funds to minimize the risk of this type of fraud. In what way does this case indicate a lack of proper segregation of duties?
6. Discuss how Greater Providence might improve its loan review procedures at bank headquarters to minimize its fraud risk. Was it a good idea to rotate the assignments of loan review clerks? Why, or why not?
7. Discuss whether Greater Providence's auditors should have been able to detect this fraud.
8. Are there any indications that the control environment at Greater Providence may have been deficient? If so, how could it have contributed to this embezzlement?

Source: John Kostrezewa, "Charge: Embezzlement," *Providence Journal-Bulletin* (July 31, 1988): F-1.

AIS in Action Solutions

QUIZ KEY

1. Verifying the validity of credit or debit card numbers during an online transaction is an example of
   a. detective controls. [Incorrect. Controls designed to discover control problems that were not prevented.]
   b. preventive controls. [Incorrect. Controls that deter problems before they arise.]
   ► **c.** application controls. [Correct. Controls that prevent, detect, and correct transaction errors and fraud in application programs.]
   d. general controls. [Incorrect. Controls designed to make sure an organization's information system and control environment is stable and well managed.]

2. Which one of the following is a key principle of the COBIT 5 framework?
   a. ensuring an approach where governance is effectively managed [Incorrect. It provides a holistic approach that ensures not only effective governance but also effective maintenance of all IT functions in the company.]
   b. focusing on IT operations [Incorrect. It does not just focus on IT operations; it integrates all IT functions and processes into company-wide functions and processes.]
   ► **c.** distinguishing between governance and management [Correct.]
   d. aligning with other standards at a low level to create a support framework for IT governance and management [Incorrect. It can be aligned at a high level with other standards and frameworks to ensure an overarching support framework for IT governance and management.]

3. Which of the following statements is true?
   a. COSO's internal control integrated framework is used to clearly define internal controls, but the evaluation of the control systems is handled elsewhere. [Incorrect. COSO's internal control integrated framework not only defines the internal controls but also provides guidance in terms of the evaluation and enhancing of internal control systems.]
   b. Control activities in COSO's internal control model focus on control activities that are performed at the management level. [Incorrect. It focuses on control activities at all levels and stages in the business process as well as technology.]
   c. The ERM model developed by COSO has a rigid three-dimensional structure that addresses four fixed management objectives, eight interrelated risk and control elements, and five subunits within each company. [Incorrect. The management objectives and the interrelated risk and control elements are necessary for the ERM model. However, the

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

five subunits are dependent on the organization itself—there may be more or less of these in a given company.]

► **d.** The ERM framework is much more comprehensive than the widely adopted IC framework. [Correct.]

4. All other things being equal, which of the following is true?

a. Detective controls are superior to preventive controls. [Incorrect. The reverse is true—preventive controls are superior to detective controls. Preventive controls keep an error or irregularity from occurring. Detective controls uncover an error or irregularity after the fact.]

b. Corrective controls are superior to preventive controls. [Incorrect. The reverse is true—preventive controls are superior to corrective controls. Preventive controls keep an error or irregularity from occurring. Corrective controls fix an error after the fact.]

c. Preventive controls are equivalent to detective controls. [Incorrect. Preventive controls keep an error or irregularity from occurring. Detective controls uncover an error or irregularity after the fact.]

► **d.** Preventive controls are superior to detective controls. [Correct. With respect to controls, it is always of utmost importance to prevent errors from occurring.]

5. Which of the following should assist management in reconciling the conflict between creativity and control?

a. measuring and monitoring actual company progress with the help of a boundary system [Incorrect. Management can measure, monitor, and compare actual company progress to the budgetary and performance goals that are previously set through a diagnostic control system.]

► **b.** using a belief system that describes how a company creates value, assists employees to understand management's vision, and inspires employees to live by those core company values [Correct.]

c. encouraging employees to attempt acting ethically by establishing boundaries on employee behavior so as to creatively solve problems [Incorrect. Employees should be helped to act ethically, not merely encouraged to attempt ethical behavior.]

d. focusing subordinates' attention on key operational issues through interactive control systems, and not interfering in their decisions [Incorrect. Managers should focus subordinates' attention on key strategic issues with the help of interactive control systems and be more involved in their decisions.]

6. To achieve effective segregation of duties, certain functions must be separated. Which of the following is the correct listing of the accounting-related functions that must be segregated?

a. control, recording, and monitoring [Incorrect. See Figure 10-4.]

► **b.** authorization, recording, and custody [Correct. See Figure 10-4.]

c. control, custody, and authorization [Incorrect. See Figure 10-4.]

d. monitoring, recording, and planning [Incorrect. See Figure 10-4.]

7. Which of the following is not an independent check?

a. bank reconciliation [Incorrect. A bank reconciliation is an independent check, as are top-level reviews, analytical reviews, reconciling two independently maintained sets of records, comparisons of actual quantities with recorded amounts, double-entry accounting, and independent reviews.]

b. periodic comparison of subsidiary ledger totals to control accounts [Incorrect. A periodic comparison of subsidiary ledger totals to control accounts is an independent check, as are top-level reviews, analytical reviews, reconciling two independently maintained sets of records, comparisons of actual quantities with recorded amounts, double-entry accounting, and independent reviews.]

c. trial balance [Incorrect. A trial balance is an independent check, as are top-level reviews, analytical reviews, reconciling two independently maintained sets of records, comparisons of actual quantities with recorded amounts, double-entry accounting, and independent reviews.]

► **d.** re-adding the total of a batch of invoices and comparing it with your first total [Correct. One person performing the same procedure twice using the same documents,

https://fliphtml5.com/pyiue/oxby/basic/301-350 38/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

such as re-adding invoice batch totals, is not an independent check because it does not involve a second person, a second set of documents or records, or a second process.]

8. Which of the following is a control procedure relating to both the design and the use of documents and records?

a. locking blank checks in a drawer [Incorrect. Locking blank checks in a drawer is not a control procedure related to the design of documents.]

b. reconciling the bank account [Incorrect. Reconciling the bank account is not a control procedure related to the design of documents.]

► **c.** sequentially prenumbering sales invoices [Correct. Designing documents so that they are sequentially prenumbered and then using them in order is a control procedure relating to both the design and the use of documents.]

d. comparing actual physical quantities with recorded amounts [Incorrect. Comparing actual quantities to recorded amounts is not a control procedure related to the design of documents.]

9. Which of the following is the correct order of the risk assessment steps discussed in this chapter?

► **a.** identify threats, estimate risk and exposure, identify controls, estimate costs and benefits [Correct. See Figure 10-3.]

b. identify controls, estimate risk and exposure, identify threats, estimate costs and benefits [Incorrect. See Figure 10-3.]

c. estimate risk and exposure, identify controls, identify threats, estimate costs and benefits [Incorrect. See Figure 10-3.]

d. estimate costs benefits, identify threats, identify controls, estimate risk and exposure [Incorrect. See Figure 10-3.]

10. Your company's current system is 85% reliable. A major threat has been identified with an impact of €7,500,000. Two possible control procedures can be implemented to deal with the identified threat. Implementation of control A would cost €45,000 and reduce the likelihood to 7%. Implementation of control B would cost €40,000 and reduce the likelihood to 4%. Implementation of both controls would cost €70,000 and reduce the likelihood to 3%. Given this information, and based solely on an economic analysis of cost and benefits, what should you do?

a. Implement control A only. [Incorrect. Control procedure A realizes a net benefit of €555,000. This is less than that of both control procedure B, which realizes a €785,000 benefit as well as that of the combination of controls A and B, which realizes the highest net benefit of €830 000.]

b. Implement control B only. [Incorrect. Control procedure B realizes a net benefit of €785,000, which is less than the benefit of the combination of both controls, which realizes a net benefit of €830,000.]

► **c.** Implement both control A and control B, [Correct. The combination of control procedures A and B realizes the highest net benefit of €830,000.]

d. Implement neither control. [Incorrect. Both controls realize a net benefit. Control procedure A realizes a net benefit of €555,000, and control procedure B realizes a net profit of €785,000 The combination of controls A and B realizes the highest net benefit of €830,000.]

Expected loss (EL):	**1125000**
Impact	**7 500 000**
Likelihood	**0.15**

Control	Likelihood	Impact	Revised EL	Reduction in EL	Cost of Control	Net Benefit (Cost)
A	0.07	7 500 000	525000	600 000	45000	555 000
B	0.04	7 500 000	300000	825 000	40000	785 000
Both	0.03	7 500 000	225000	900 000	70 000	830 000

https://fliphtml5.com/pyiue/oxby/basic/301-350 39/45

CHAPTER

11

Controls for Information Security

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

1. Explain how security and the other four principles in the Trust Services Framework affect systems reliability.
2. Explain three fundamental concepts: why information security is a management issue, how people's behavior impacts security, and the time-based model of information security.
3. Describe the controls that can be used to protect an organization's information.
4. Describe the controls that can be used to timely detect that an organization's information system is under attack.
5. Discuss how organizations can timely respond to attacks against their information system.
6. Explain how virtualization, cloud computing, and the Internet of Things affect information security.

INTEGRATIVE CASE Northwest Industries

Jason Scott's next assignment is to review the internal controls over Northwest Industries' information systems. Jason obtains a copy of COBIT 2019 and is impressed by its thoroughness. However, he tells his friend that he feels overwhelmed in trying to use COBIT 2019 to plan his audit of Northwest Industries. His friend suggests that he examine the Trust Services Framework developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) to guide auditors in assessing the reliability of an organization's information system and to perform attestation services related to cybersecurity. After reviewing the framework, Jason concludes that he can use it to guide his audit effort. He decides that he will begin by focusing on the controls designed to provide

FuzzBones/Shutterstock

reasonable assurance about information security. He writes down the following questions that will guide his investigation:

1. What controls does Northwest Industries employ to prevent unauthorized access to its accounting system?
2. How can successful and unsuccessful attempts to compromise the company's accounting system be detected in a timely manner?
3. What procedures are in place to respond to security incidents?

Introduction

Management wants assurance that the information produced by the organization's own accounting system is reliable. Management also wants assurance about the reliability of the cloud service providers with whom it contracts. Finally, management wants assurance that the organization is compliant with an ever-increasing array of regulatory and industry requirements, including Sarbanes–Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and updates to it in the Health Information Technology for Economic and Clinical Health Act (HITECH), the EU's General Data Privacy Regulation (GDPR), and the Payment Card Industry Data Security Standards (PCI-DSS).

As noted in Chapter 10, COBIT 2019 is a comprehensive framework of best practices relating to all aspects of the governance and management of IT. However, in this book we focus on only those portions of COBIT 2019 that most directly pertain to the reliability of an information system and compliance with regulatory standards. Consequently, we organize this chapter and the next two around the principles in the Trust Services Framework, which was developed jointly by the AICPA and the CICA to provide guidance for assessing the reliability of information systems. Nevertheless, because COBIT 2019 is an internationally recognized framework used by many organizations, auditors and accountants need to be familiar with it. Therefore, throughout our discussion we reference the relevant sections of COBIT 2019 that relate to each topic so that you can understand how the principles that contribute to systems reliability are also essential to effectively managing an organization's investment in IT.

The Trust Services Framework organizes IT-related controls into five principles that jointly contribute to systems reliability:

1. ***Security***—access (both physical and logical) to the system and its data is controlled and restricted to legitimate users.
2. ***Confidentiality***—sensitive organizational information (e.g., marketing plans, trade secrets) is protected from unauthorized disclosure.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

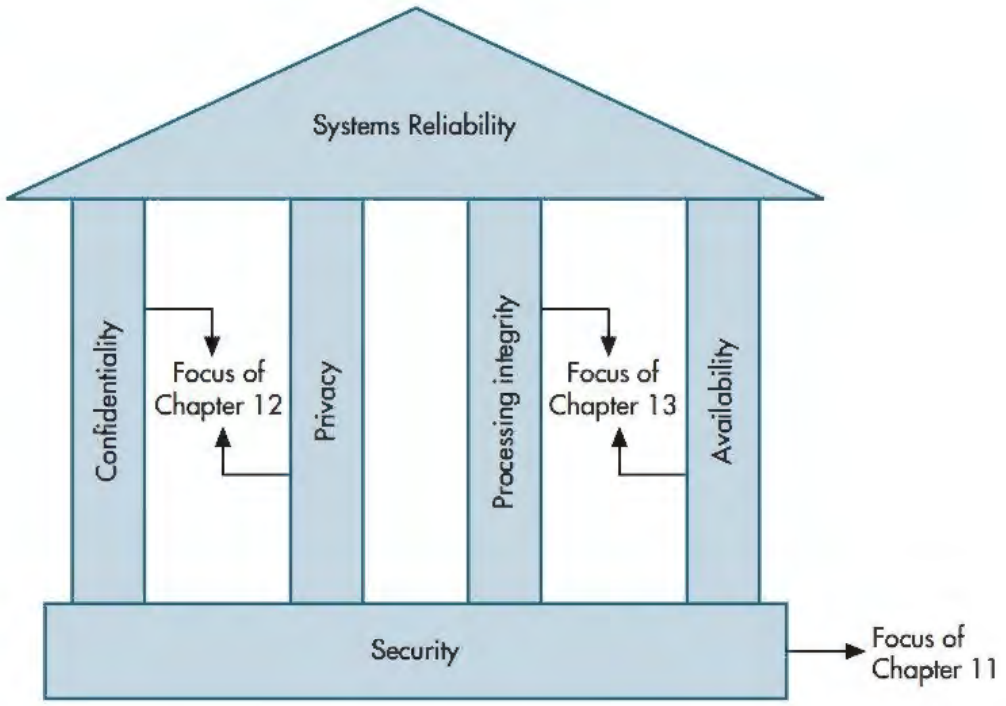


FIGURE 11-1
Relationships Among the Five Trust Services Principles for Systems Reliability

3. ***Privacy***—personal information about customers, employees, suppliers, or business partners is collected, used, disclosed, and maintained only in compliance with internal policies and external regulatory requirements and is protected from unauthorized disclosure.
4. ***Processing Integrity***—data are processed accurately, completely, in a timely manner, and only with proper authorization.
5. ***Availability***—the system and its information are available to meet operational and contractual obligations.

As Figure 11-1 shows, information security is the foundation of systems reliability and is necessary for achieving each of the other four principles. Information security procedures restrict system access to authorized users only, thereby protecting the confidentiality of sensitive organizational data and the privacy of personal information collected from customers. Information security procedures protect information integrity by preventing submission of unauthorized or fictitious transactions and preventing unauthorized changes to stored data or programs. Finally, information security procedures provide protection against a variety of attacks, including viruses and worms, thereby ensuring that the system is available when needed. This chapter focuses on information security. Chapter 12 discusses the IT controls relevant to protecting the confidentiality of an organization's intellectual property and the privacy of information it collects about its customers and business partners. Chapter 13 then covers the IT controls designed to ensure the integrity and availability of the information produced by an organization's accounting system.

Three Fundamental Information Security Concepts

1. SECURITY IS A MANAGEMENT ISSUE, NOT JUST A TECHNOLOGY ISSUE

Although effective information security requires the deployment of technological tools such as firewalls, antivirus, and encryption, senior management involvement and support throughout all phases of the security life cycle (see Figure 11-2) is absolutely essential for success. The first step in the security life cycle is to assess the information security-related threats that the organization faces and select an appropriate response. Information security professionals possess the expertise to identify potential threats and to estimate their likelihood and impact. However, senior management must choose which of the four risk responses described in Chapter 10 (reduce, accept, share, or avoid) is appropriate to adopt so that the resources invested in information security reflect the organization's risk appetite.

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

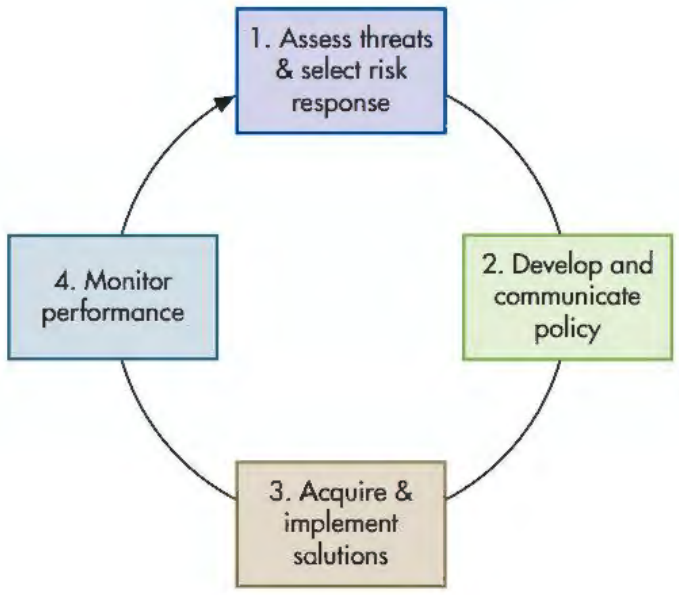

1. Assess threats & select risk response
2. Develop and communicate policy
3. Acquire & implement solutions
4. Monitor performance

FIGURE 11-2
The Security Life Cycle

Step 2 involves developing information security policies and communicating them to all employees. Senior management must participate in developing policies because they must decide the sanctions they are willing to impose for noncompliance. In addition, the active support and involvement of top management is necessary to ensure that information security training and communication are taken seriously. To be effective, this communication must involve more than just handing people a written document or sending them an e-mail and asking them to sign an acknowledgment that they received and read the notice. Instead, employees must receive regular, periodic reminders about security policies and training on how to comply with them.

Step 3 of the security life cycle involves the acquisition or building of specific technological tools. Senior management must authorize investing the necessary resources to mitigate the threats identified and achieve the desired level of security. Finally, step 4 in the security life cycle entails regular monitoring of performance to evaluate the effectiveness of the organization's information security program. Advances in IT create new threats and alter the risks associated with old threats. Therefore, management must periodically reassess the organization's risk response and, when necessary, make changes to information security policies and invest in new solutions to ensure that the organization's information security efforts support its business strategy in a manner consistent with management's risk appetite.

Many functions play a role in implementing an organization's information security program. The information technology function is responsible for installing and maintaining the various technological solutions. The risk and compliance group must work with management to design policies to ensure compliance with various regulations about security and privacy. All employees with access to the system need to understand and comply with security policies. Information security professionals have expertise in information security and regularly monitor those solutions to be sure they function effectively as well as monitor compliance with policies. The internal audit function periodically performs an independent review of the efficiency and effectiveness of the organization's information security program.

The fact that multiple functions are involved in information security is another reason why security is an important issue for senior management. First, whenever multiple organizational functions or groups deal with a common issue, there is the possibility that a lack of effective communication will result in separate "silos" so that each function approaches their task without coordinating with the work of the other groups. A second and even more dysfunctional potential problem whenever multiple organizational functions share responsibility for a task is a lack of cooperation and "turf" battles. Only senior management's involvement can overcome these two potential problems. Focus 11-1 summarizes recent research that finds that not only does senior management involvement in and support for information security mitigate those potential problems, but it actually improves the overall effectiveness of the organization's information security program.

https://fliphtml5.com/pyiue/oxby/basic/301-350 43/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

FOCUS 11-1 How Senior Management Can Improve the Organization's Information Security

Research indicates that top management needs to demonstrate their support for information security by exhibiting the following behaviors:

- Provide adequate resources for information security.
- Regularly communicate the importance of information security.
- Demonstrate, by their actions, that they believe information security is important.
- Adopting a proactive approach to potential security threats, instead of reacting to problems after they happen.
- Including information security issues whenever assessing the risk of any new initiative.

Doing so creates a "security-aware" organizational culture in which all employees believe information security is important. As a result, employee compliance with security policies increases. Visible top management support for information security also improves the design of internal controls, reducing the number of security-related weaknesses.

But perhaps the most important result of top management support for information security is that it improves the relationship between the information security and internal audit functions, reducing "turf" battles between the functions and increasing the sharing of information between them. This is important because a better relationship between those two functions improves security in a number of ways, including:

1. Increased detection of attacks *before* they cause material harm to the organization. This is the ultimate objective of security.
2. More timely detection of attacks after they have caused harm. This is important because you cannot "stop the bleeding" until you know you have a cut. The magnitude of the damage caused by many of the major security breaches in recent years is partly because the affected organizations did not even know they had been attacked for months or even years.
3. Improved ability to detect serious issues involving employee noncompliance with security policies. Security policies are designed to reduce risk; conversely, noncompliance with those policies increases the risk that employee action (or inaction) will result in a security incident. More timely detection of noncompliance enables managers to take countermeasures and better enforce compliance with policies.
4. Improved ability to detect security-related material internal control weaknesses. Such weaknesses represent vulnerabilities that attackers can exploit. More timely detection enables organizations to remedy those vulnerabilities.

Source: Steinbart, P. J., R. L. Raschke, G. Gal, & W. N. Dilla. 2018. "The Influence of a good relationship between the internal audit and information security functions on information security outcomes," *Accounting, Organizations and Society* 71: pp. 15–29.

2. PEOPLE: THE CRITICAL FACTOR

People can either be the "weakest link" in security or an important asset. To make employees a positive part of the organization's security efforts, management must create a "security-conscious" culture and provide continuous security awareness training. The discussion of the COSO framework in Chapter 10 stressed how top management's risk attitudes and behaviors create either an internal environment that supports and reinforces sound internal control or one that effectively negates written control policies. The same principle holds regarding information security. Indeed, both COBIT 2019 and the Trust Services Framework specifically identify an organization's culture and ethics as one of the critical enablers for effective information security. To create a security-conscious culture in which employees comply with organizational policies, top management must not only communicate the organization's security policies, but must also lead by example. Employees are more likely to comply with information security policies when they see their managers do so. Conversely, if employees observe managers violating an information security policy, for example by writing down a password and affixing it to a monitor, they are likely to imitate that behavior.

Employee skills and competencies are another critical enabler for effective information security. Employees must understand how to follow the organization's security policies. The importance of training is reflected in the fact that security awareness training is discussed as a key practice to support several of COBIT 2019's 35 management processes. It is especially important to train new employees because criminals often target newly hired employees with sophisticated phishing emails.

https://fliphtml5.com/pyiue/oxby/basic/301-350 44/45

23/2/23, 20:32 Marshall B. Romney - Accounting information systems-Pearson Education Limited (2021) - 9781292353364 Pages 301-350 - Flip PDF Download | FlipHTML5

All employees should be taught *why* security measures are important to the organization's long-run survival. They also need to be trained to follow safe computing practices, such as never opening unsolicited e-mail attachments, using only approved software, not sharing passwords, and taking steps to physically protect laptops. Training is especially needed to educate employees about social engineering attacks. For example, employees should be taught never to divulge passwords or other information about their accounts or their workstation configurations to anyone who contacts them by telephone, e-mail, or instant messaging and claims to be part of the organization's information systems security function. Employees also need to be trained not to allow other people to follow them through restricted access entrances. This social engineering attack, called *piggybacking*, can take place not only at the main entrance to the building but also at any internal locked doors, especially to rooms that contain computer equipment. Piggybacking may be attempted not only by outsiders but also by other employees who are not authorized to enter a particular area. Piggybacking often succeeds because many people feel it is rude to not let another person come through the door with them or because they want to avoid confrontations. Role-playing exercises are particularly effective for increasing sensitivity to and skills for dealing with social engineering attacks.

Security awareness training is also important for senior management because in recent years many social engineering attacks, such as spear phishing, have been targeted at them. Thus far, the discussion of training has focused on the protection component of the time-based model of security by teaching employees and managers how to prevent problems. But training can also improve both timely detection and response if both employees and managers are trained not only to avoid certain behaviors, but also to promptly notify information security whenever they receive suspicious emails or other forms of social engineering.

However, an organization's investment in security training will be effective only if management clearly demonstrates that it supports employees who follow prescribed security policies. This is especially important for combating social engineering attacks because countermeasures may sometimes create embarrassing confrontations with other employees. For example, one of the authors heard an anecdote about a systems professional at a major bank who refused to allow a person who was not on the list of authorized employees to enter the room housing the servers that contained the bank's key financial information. The person denied entry happened to be a new executive who was just hired. Instead of reprimanding the employee, the executive demonstrated the bank's commitment to and support for strong security by writing a formal letter of commendation for meritorious performance to be placed in the employee's performance file. It is this type of visible top management support for security that enhances the effectiveness of all security policies. Top management also needs to support the enforcement of penalties, up to and including dismissal, against employees who willfully violate security policies. Doing so not only sends a strong message to other employees but also may sometimes lessen the consequences to the organization if an employee engages in illegal behavior. Training of information security professionals is also important. New developments in technology continuously create new security threats and make old solutions obsolete. Therefore, it is important for organizations to support continuing professional education for their security specialists.

3. THE TIME-BASED MODEL OF INFORMATION SECURITY

The goal of the **time-based model of information security** is to employ a combination of preventive, detective, and corrective controls to protect information assets long enough for an organization to detect that an attack is occurring and to take timely steps to thwart the attack before any information is lost or compromised. The time-based model of information security can be expressed in the following formula:

time-based model of information security - Implementing a combination of preventive, detective, and corrective controls that protect information assets long enough to enable an organization to recognize that an attack is occurring and take steps to thwart it before any information is lost or compromised.

$$P > D + R, \text{ where}$$

P = the time it takes an attacker to break through the various controls that protect the organization's information assets.
D = the time it takes for the organization to detect that an attack is in progress.
R = the time it takes to respond to and stop the attack.

If the equation is satisfied (i.e., if $P > D + R$ is true), then the organization's information security procedures are effective. Otherwise, security is ineffective.